فهرست مطالب

فصل اول : مبانی فرکانس رادیویی (RF) ۳

مبانی Radio Frequency (RF) ۴

رفتار RF ۴

در ادامه بحث ، رفتار های مختلف Radio Frequency را در محیط بررسی می نماییم ۴

فصل دوم : اجزاء RF ، ریاضیات و محاسبات ۹

Intentional Radiator ۱۰

Equivalent Isotropically Radiated Power (EIRP) ۱۰

ریاضیات RF ۱۱

فصل سوم : آنتن ها و سیگنال های RF ۱۲

Gain و Beamwidth در آنتن ۱۳

انواع آنتن ۱۴

آنتن های Omni-Directional (Dipole) ۱۴

آنتن هایSemi-Directional ۱۶

آنتن های Highly-Directional ۱۷

Polarization ۱۹

Voltage Standing Wave Ratio (VSWR) ۲۰

دستگاه های جانبی Wireless ۲۲

Power over Ethernet (PoE) ۲۷

فصل چهارم : سازمان ها و استانداردهای وایرلس ۲۹

استاندارد ها و سازمان ها ۳۰

قوانین میزان Power (FCC) ۳۱

استاندارد های IEEE در مقابل European Telecom Standard Institute : ۳۲

Cisco in Persian

سری استاندارد های IEEE 802.11 ..... ۳۲
استاندارد IEEE 802.11i ۳۴
استاندارد 802.16 ..... ۳۷

فصل پنجم : شبکه های وایرلس و تکنیک های Spread Spectrum ۳۹

تکنیک Spread Spectrum ۴۰
FHSS (Frequency Hopping Spread Spectrum) ۴۱
DSSS (Direct Sequence Spread Spectrum) ۴۲

فصل ششم : ساختار شبکه ی 802.11 ..... ۴۳

SSID & Beacon ۴۳
SSID & Beacons ۴۴
Passive Scanning ۴۵
Active Scanning ۴۵
Authentication و Association ۴۶
Roaming ۴۸
توپولوژی های 802.11 - انواع Service Set ۵۱

فصل هفتم : تجهیزات وایرلس ۵۳

انواع Access Point ۵۴
انواع Wireless Bridge ۵۶
Wireless Workgroup Bridge ۵۸
Wireless Residential Gateway ۵۸
Wireless LAN Clients ۵۸

فصل هشتم : WLAN Deployment و کاربردهای آن ۵۹

کاربرد ها ۶۰

Cisco in Persian

فصل اول : مبانی فرکانس رادیویی (RF)

- ❖ مبانی RF
- ❖ رفتار RF
  - ✓ Gain (Amplification)
  - ✓ Loss (Attenuation)
  - ✓ Reflection
  - ✓ Refraction
  - ✓ Diffraction
  - ✓ Scattering
  - ✓ Absorption

Cisco in Persian

مبانی Radio Frequency (RF)

فرکانسهای رادیویی در واقع سیگنال های High Frequency Alternating Current (AC) هستند که بعد از عبور از سیم رسانا ، توسط آنتن به هوا متشعشع می شوند. در واقع آنتن مبدل (Converter/Transformer) یک سیگنال سیمی به سیگنال بی سیم (و بالعکس) است. وقتی سیگنال AC روی هوا تشعشع می شود ، بشکل امواج رادیویی در می آید . این امواج از مبدا (آنتن) در همه جهات بصورت مستقیم ، به یکباره حرکت می کنند و پخش میشوند ؛ مثل پرتاب سنگ به آب ساکن و آرام ، و ایجاد موج های حاصله و حرکت آنها .

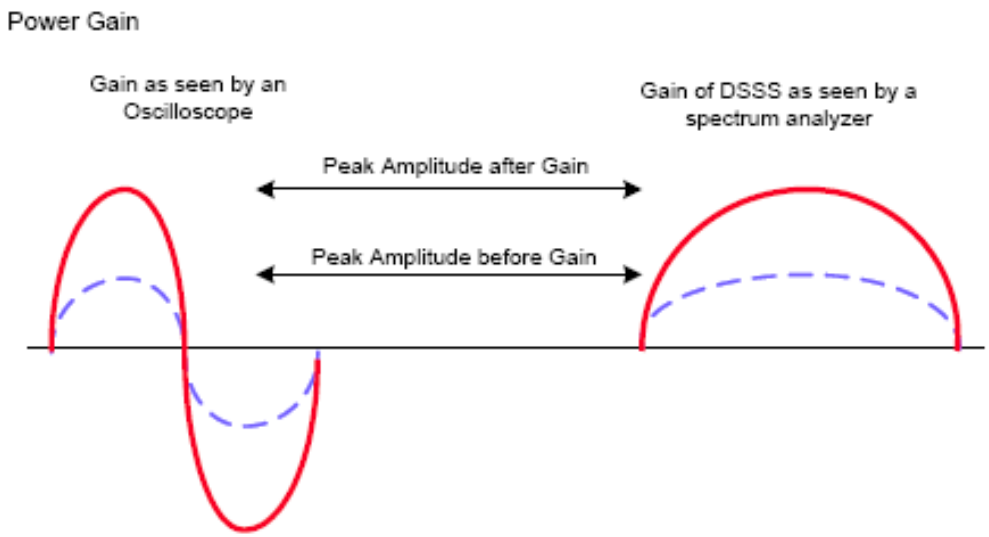
رفتار RF

پس از این مقدمه، به رفتار های مختلف Radio Frequency را در محیط میپردازیم:

Gain

به افزایش دامنه سیگنال گویند و در واقع فرایندی Active است ؛ یعنی سیگنال توسط منبع تغذیه (Power Source) خارجی (و یا توسط یک آنتن High-gain) ، همانند یک آمپلی فایر (RF Amplifier) تقویت می شود .

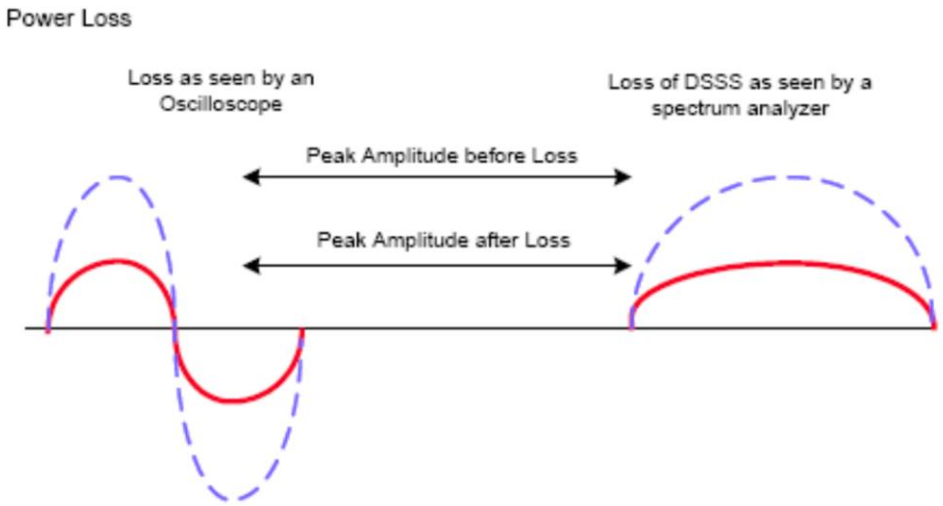
البته یک فرایند Passive نیز می تواند موجب Gain شود . مثلا ترکیب سیگنالهای منعکس شده بهمراه سیگنال اصلی موجب تقویت سیگنال اصلی می شود . عموما به غیر از موارد خاص ، هرچه سیگنال قویتر باشد بهتر است .



Cisco in Persian

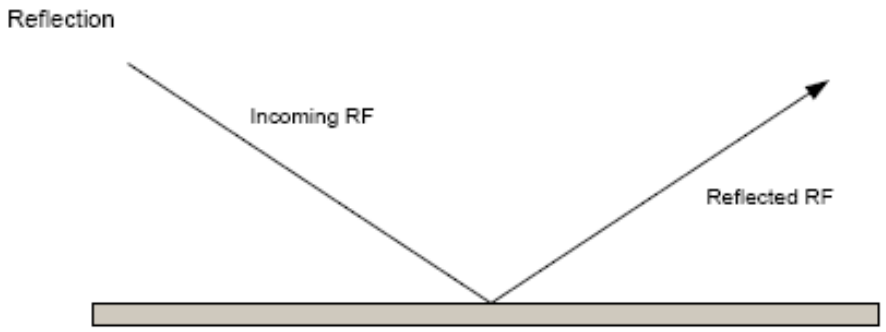
Loss

کاهش مقدار قدرت سیگنال را Loss می گویند. این Loss عوامل بسیار زیادی می تواند داشته باشد، مثل مقاومت غیر همسان کابل و کانکتور که موجب برگشت سیگنال و در نتیجه کاهش قدرت سیگنال می شود. Loss چه در کابل و یا هوا ممکن است اتفاق بیافتد. بطور مثال بسته به مانعی که سر راه سیگنال است، ممکن است موجب جذب، انعکاس، و یا حتی تخریب سیگنال شود. در برخی از موارد Loss را عمدا بوجود می آورند و این کار در جهت کاستن از قدرت سیگنال در نقاط خاص توسط Attenuator انجام میگیرد.



Reflection

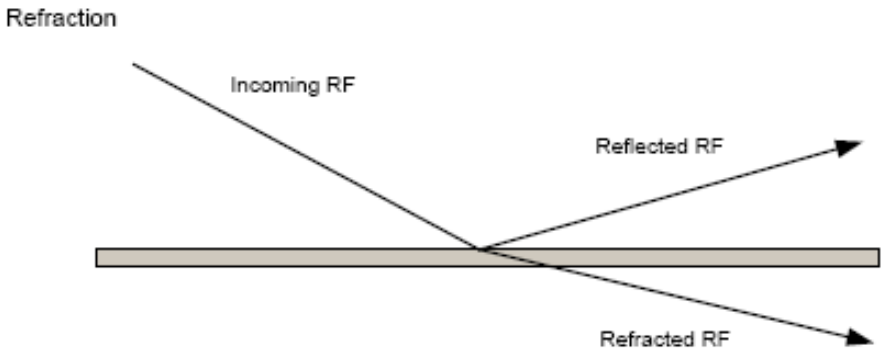
وقتی موج الکترومغناطیسی به جسمی با ابعاد بزرگ (نسبت به طول موج) برخورد کند ، منعکس شده و تغییر جهت می دهد . انعکاس عموما در برخورد با سطح زمین ، ساختمان ، دیوار و یا هر مانع دیگر روی می دهد . هر چه سطح صاف و صیقلی تر باشد ، موج منعکس شده سالم تر می ماند . انعکاس ممکن است موجب بروز مشکلاتی گردد ؛ در واقع انعکاس چندباره ی سیگنال اصلی بر اساس برخورد با اجسام متعدد در ناحیه انتقال ، Multipath نامیده می شود و موجب تضعیف ، تباه شدن و یا ایجاد رخنه و سیگنال بریده بریده شود(در سطوحی نظیر دریاچه یا استخر ، سقف فلزی ، در و دیوار فلزی و غیره) . برای حل این مشکل ، می توان از سخت افزارهای مخصوصی (مثل انواع آنتن ها) استفاده کرد .



Cisco in Persian

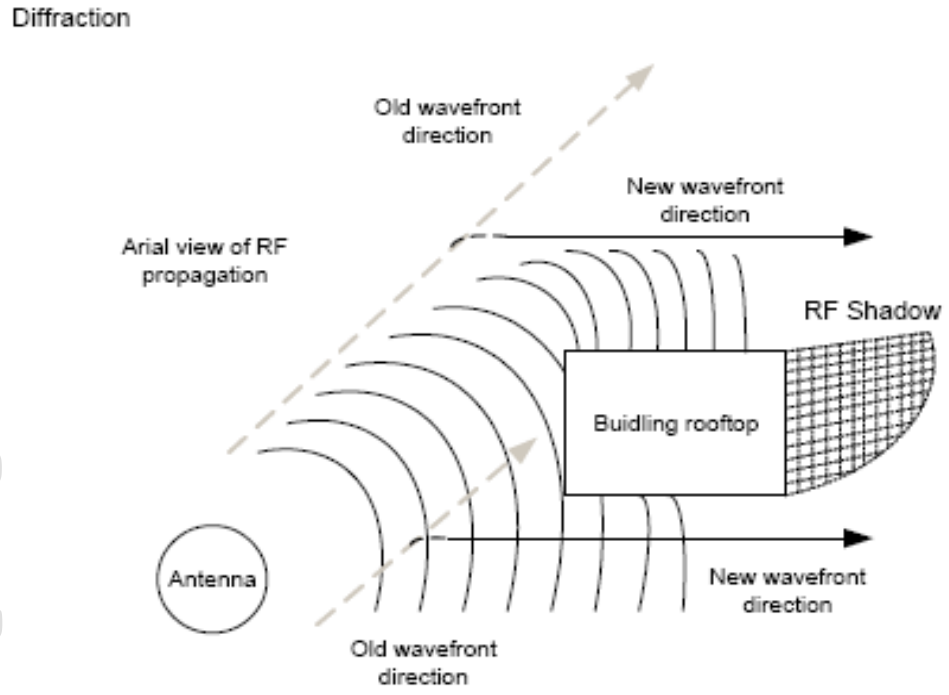
Refraction

به انحراف سیگنال ، وقتی از رسانه ای به رسانه دیگر (تغییر چگالی) وارد می شود ، refraction می گویند . وقتی موج به رسانه متراکم تر می رسد (مثل هوای سرد میانکوه) ، دچار انحراف زاویه می شود . این مشکل اغلب در لینک های با فاصله طولانی اتفاق می افتد (تغییر اتموسفر و شرایط جوی).



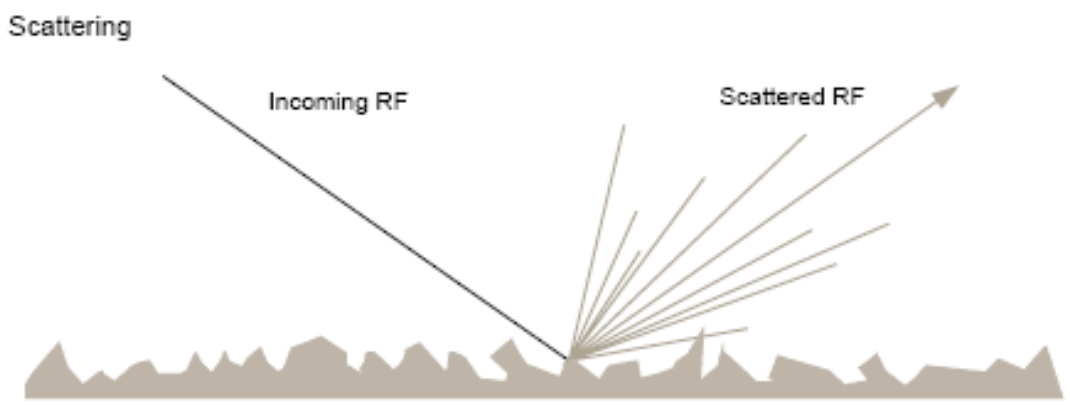
Diffraction

Diffraction به انحراف سیگنال نسبت به اطراف یک مانع (بشکل نامعمول و ناهنجار) و ایجاد خمیدگی موج گفته می شود ؛ در حالیکه Refraction به انحراف سیگنال در داخل خود مدیا اشاره می کند .



Scattering

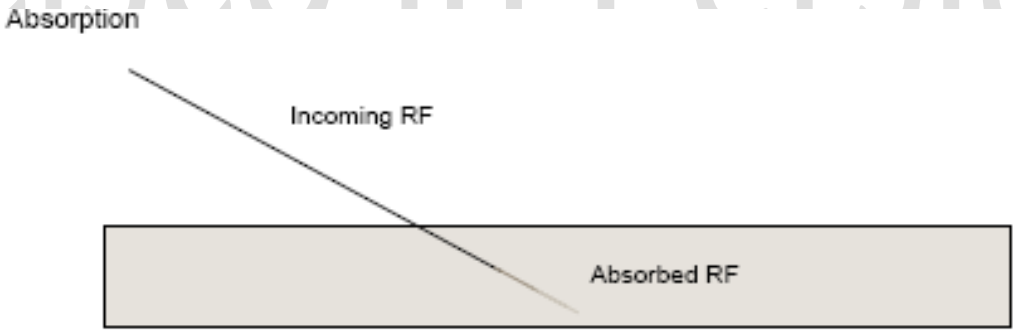
پراکندگی در برخورد با سطحی زبر که دارای ناهمواری های ریز (نسبت به طول موج) است و منجر به انعکاس موج به چندین زاویه به ازای هر برآمدگی ناهموار می شود ، scattering نام دارد . نوع دیگر این پراکندگی ، می تواند برخورد موج با گرد وغبار و اجسام ریز معلق در هوا دانست .



Absorption

Cisco in Persian

جذب سیگنال زمانی اتفاق می افتد که موج RF به شیئی برخورد می کند ، اما نه منعکس شده ، نه از آن عبور میکند و نه منحرف می شود .



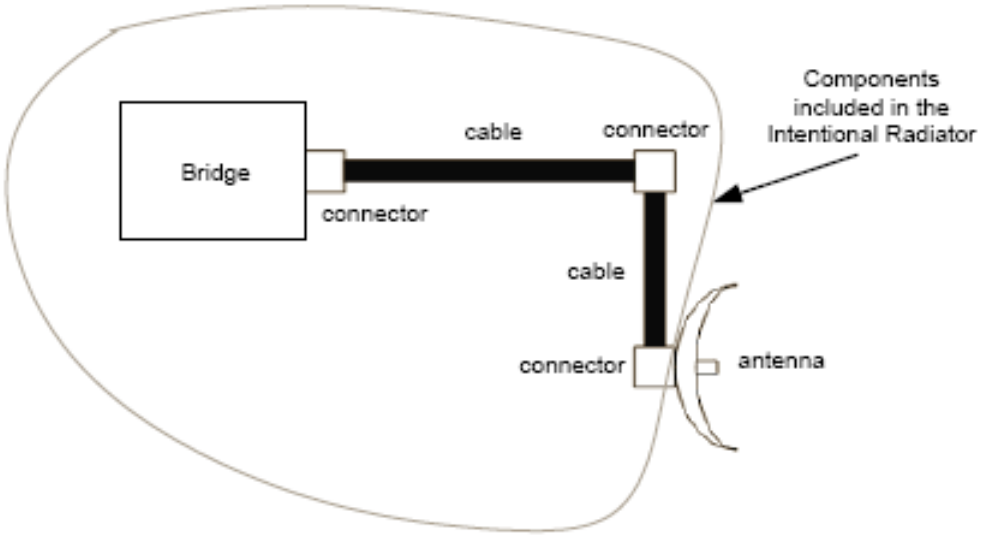
فصل دوم : اجزاء RF ، ریاضیات و محاسبات

Cisco in Persian

- ❖ Intentional Radiator
- ❖ Equivalent Isotropically Radiated Power (EIRP)
- ❖ ریاضیات RF

Intentional Radiator

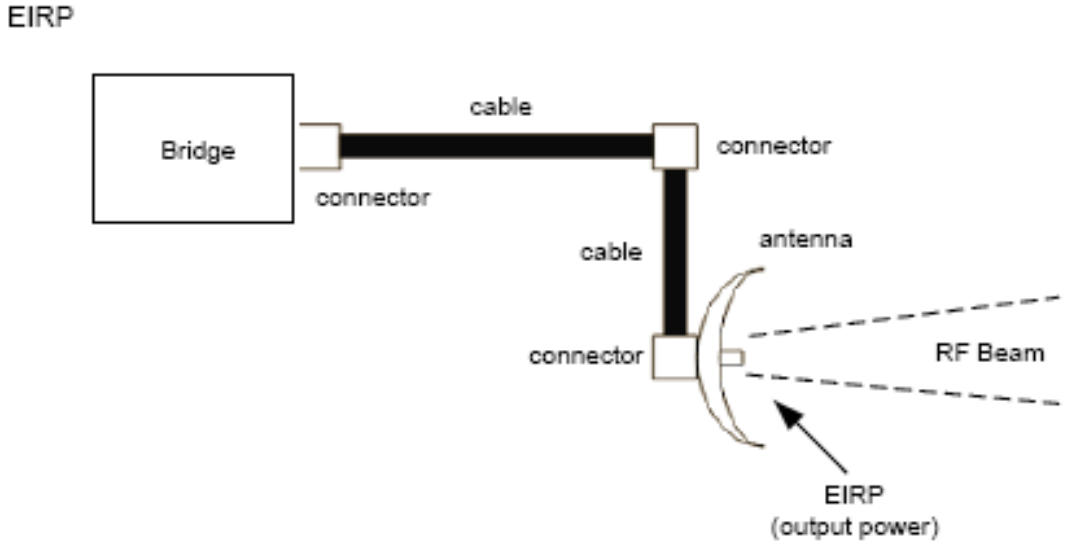
طبق تعریف Federal Communication Commission (FCC) ، به دستگاهی از RF می گویند که وظیفه ایجاد و تشعشع سیگنال های RF را دارد . به دید سخت افزاری ، این تعریف خود شامل کل دستگاه RF و کابل ها (به غیر از آنتن) می شود . هرجا صحبت از Power Output of Intentional Radiator می شود ، منظور Power در آخرین کابل خروجی به آنتن است .



Cisco in Persian

Equivalent Isotropically Radiated Power (EIRP)

EIRP، توانی است که از آنتن تابانیده می شود و حاصل مجموع قدرت همراه با محاسبه Gain یک آنتن میباشد .



ریاضیات RF

برای محاسبه قدرت از وات (Watt) و دسیبل (dB) استفاده میکنیم . Watt مقیاسی خطی است و می تواند صفر باشد ؛ در حالیکه مقیاس dB نسبی و لگاریتمی است و نمی تواند صفر باشد. برای ارتباط دادن dB به Watt ، از dBm استفاده می کنیم بطوریکه داریم :

1 mW = 0 dBm

مثلا :

10 mW + 3dB = 20 mW

100 mW – 3dB = 50 mW

10 mW + 10dB = 100 mW

300 mW – 10dB = 30 mW

-3 dB = half the power in mW
+3 dB = double the power in mW
-10 dB = one tenth the power in mW
+10 dB = ten times the power in mW

Cisco in Persian

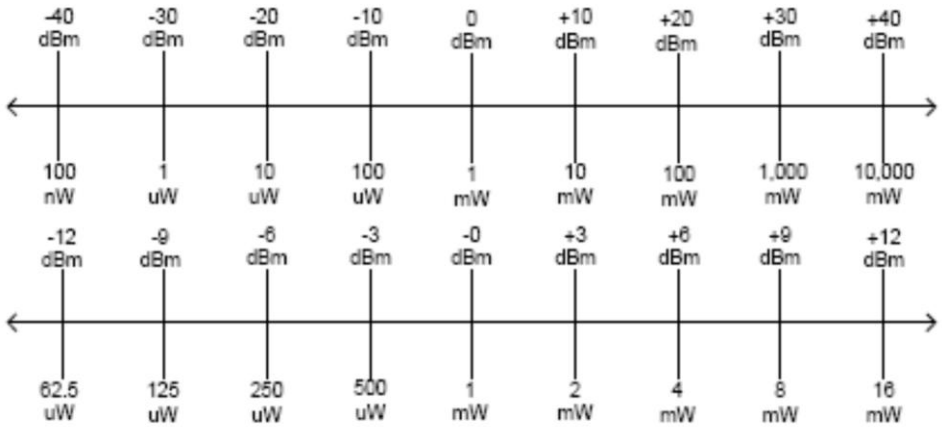
$$P_{dbm} = 10\log_{PmW}$$

$$Pmw = \log^{-1}\left(\frac{P_{dbm}}{10}\right)$$

برای خطی کردن مقیاس دسیبل (چون نسبی است) در محاسبه Gain آنتن ها از dBi استفاده می شود.

یعنی هر بار که ۳ dBi افزوده شود Power دو برابر و اگر3dBi کم شود Power نصف می شود در حالیکه اگر 10dBi افزوده شود ۱۰ برابر می شود! چون لگاریتمی است.

Power level chart



فصل سوم : آنتن ها و سیگنال های RF

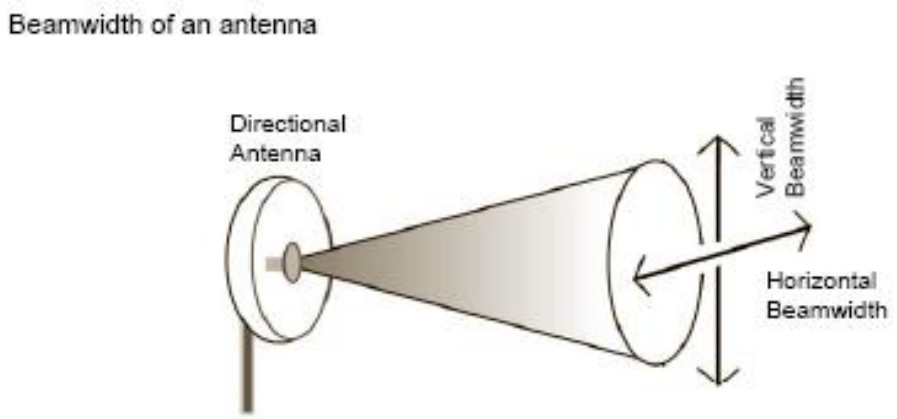
- ❖ Gain و پهنای Beam در آنتن
- ❖ انواع آنتن ها
  - ✓ Omnidirectional
  - ✓ Semidirectional
  - ✓ Highly directional
- ❖ Line Of Sight
- ❖ Fresnel Zone
- ❖ Polarization
- ❖ Voltage Standing Wave Ratio
- ❖ مثال کاربردی در مورد آنتن ها
- ❖ تجهیزات و دستگاههای جانبی Wireless
  - ✓ Amplifier
  - ✓ Attenuator
  - ✓ Lightning Arrestor
  - ✓ Splitter
  - ✓ Connectors
  - ✓ Cables
  - ✓ Frequency Converter
  - ✓ Test Kits
  - ✓ مبدل Power Over Ethernet

Cisco in Persian

Gain و Beamwidth در آنتن

یک آنتن (بدون در نظرگرفتن آمپلی فایر و فیلتر) یک دستگاه Passive است و هیچ تغییری در قدرت سیگنال ورودی ایجاد نمی کند ؛ اما با استفاده از شکل و خاصیت فیزیکی خود می تواند موجب افزایش قدرت سیگنال شود (هر چه RF را به Beam و پرتو باریکتر جلو ببرد ، بیشتر متمرکز شده (مثل پرتو باریک نور) و به برد آن می افزاید).

در واقع با تغییر Beamwidth که توسط زوایای Horizontal و Vertical اندازه گیری می شود ، این کار صورت می گیرد . بطور مثال ، یک آنتن Omni-Directional که ۳۶۰ درجه افقی Beamwidth (Horizontal) دارد، با محدود شدن به ۳۰ درجه و در یک جهت (با قدرت یکسان) مسیر بیشتری را طی میکند.



ما نمی توانیم یک Isotropic Radiator بسازیم (کره ای که تشعشع همگرا و یکسان به همه سو با قدرت مساوی و در یک زمان دارد ؛ مثل خورشید) ؛ اما می توانیم آنتن Omni-Directional ی بسازیم که در ۳۶۰ درجه افقی امواج را منتشر کند (یعنی فقط Horizontal و نه در ۳۶۰ درجه Vertical) . هر چه Gain آن را بیشتر کنیم ، افقی تر و کشیده تر می شود .

Gain یک آنتن با dBi نشان داده می شود (به معنی دسیبل در واحد یک isotropic radiator). درازا ، باریکی ، تمرکز و Focus Beam یک آنتن موجب افزایش Gain در آنتن می شود و به اندازه آن Beamwidth می گویند که با دو بردار Vertical و Horizontal و زاویه آنها مشخص می شود . آنتن ها دارای Beamwidth مختلف هستند :

نوع آنتن	درجه Horizontal Beamwidth	درجه Vertical Beamwidth
Omni-Directional	360	7~80
Patch/Panel	30~180	6~90
Yagi	30~78	14~64
Parabolic	4~25	4~21

انواع آنتن

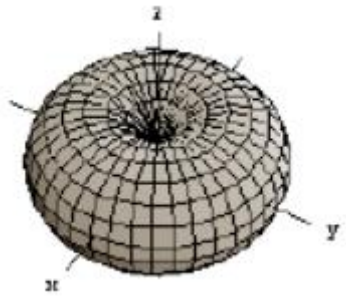
نقش آنتن، تبدیل انرژی الکتریکی به امواج RF در فرستنده و متقابلا تبدیل امواج RF به انرژی الکتریکی در گیرنده است . اندازه فیزیکی یک آنتن (مثل طول) مستقیما مرتبط با فرکانس ارسال و دریافت آن می باشد .

آنتن های Omni-Directional (Dipole)

آنتن استاندارد نصب شده روی APها ، Dipole است . آنتن های Dipole دارای قسمتی بطول یک اینچ هستند که امواج را به اطراف محور ارسال می کنند ؛ مثل آنتنهای گیرنده تلویزیون که بصورت گوش خرگوش (Rabbit Ear) هستند ؛ در حالیکه بسیار کوچکتر از آنتن های 100 MHz ی تلویزیون هستند . Dipole همانند آنتن های Omni-Directional انرژی را در قیف مانندی بنام beam متمرکز می کند . هر چه فرکانس بالاتر رود ، طول موج و آنتن کوچکتر می شوند .

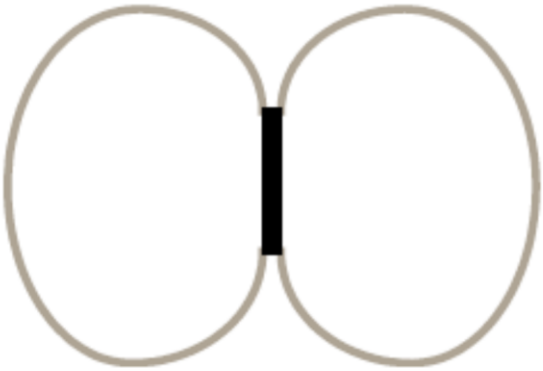
Dipole در همه جهات امواج را منتشر می کند غیر از راستای کابل خودش (بشکل شیرینی حلقه ای توخالی) و بصورت افقی تمام ۳۶۰ درجه پیرامون خود را پوشش می دهد اما مقدار کمی از بالا و پایین خود را نیز شامل می شود و هر چه Gain آنرا بیشتر کنیم ، خمیده تر و پوشش افقی آن بهتر شده ، اما از پوشش عمودی آن کاسته می شود .

Cisco in Persian



اگر Dipole را در طبقه از ساختمان قرار دهیم، سیگنال همان طبقه را بصورت افقی بهتر پوشش می دهد تا طبقات بالایی یا پایینی . به همین دلیل در ارتباط PTMP (Point to Multi-point) کاربرد وسیعی دارد . برای مصارف Indoor بهتر است در مرکز محوطه مورد نظر و نزدیک سقف قرار گیرد.

Dipole side-view

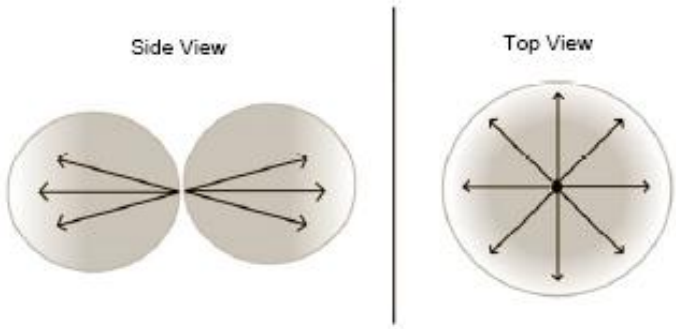


انواع آنتن

•

- Omni Ground Plane Antenna
- Omni Ceiling Mount Antenna

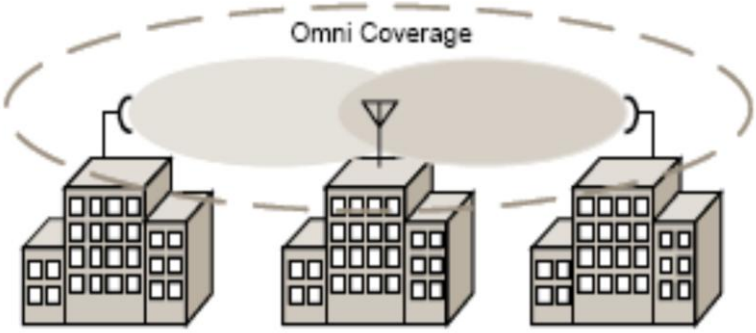
Coverage area of an omni-directional antenna



Cisco in Persian

Coverage area of a high-gain omni-directional antenna

Point-to-multipoint link



آنتن هایSemi-Directional

این گونه از آنتن ها برای برقراری لینک های Point to Point (فواصل کوتاه تا متوسط) و همچنین مصارف Indoor با قرارگیری در گوشه مناسب هستند .

Point-to-point link using semi-directional antennas

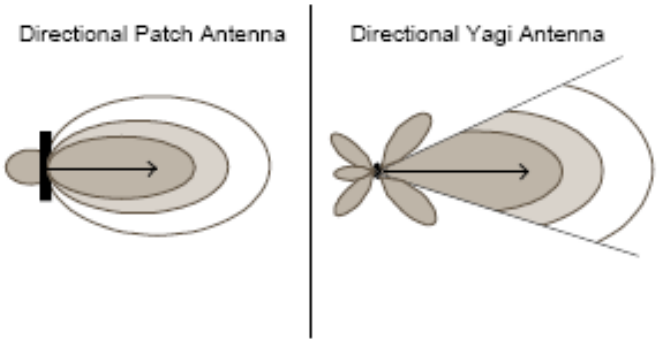
گاهی بجای استفاده از چند AP بهتر است از یک یا دو آنتن Semi-Directional استفاده کرد که موجب پوشش بهتر و صرفه جویی در هزینه می شود . از انواع این آنتن می توان موارد زیر را نام برد :

- Yagi Antenna
- Patch Antenna
- Panel Antenna

Sample semi-directional antennas

Yagi Antenna Patch Antenna Panel Antenna

Coverage area of a semi-directional antenna



آنتن های Highly-Directional

سیگنال های حاصل از این آنتن ها باریکتر و متمرکزترند (High-Gain) و فقط برای مصارف PtP بین ۲۵ تا ۴۰ کیلومتر مناسبند و باید بخوبی نصب شوند .

Radiation pattern of a highly-directional antenna

از انواع آین آنتن می توان به موارد زیر اشاره کرد:

- Highly-Directional Grid Antenna
- Highly-Directional Parabolic

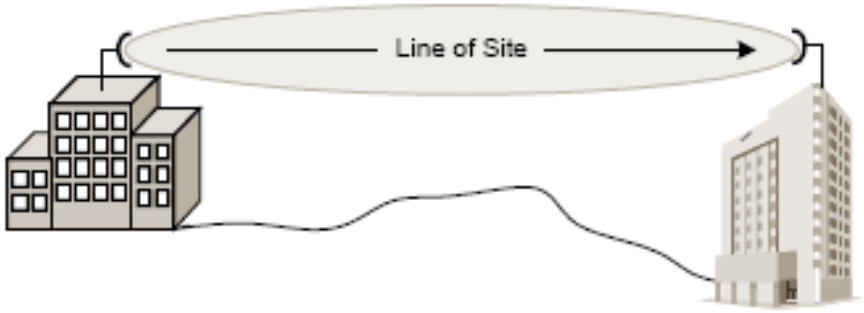
Sample of a highly-directional parabolic dish antenna

Sample of a highly-directional grid antenna

مسیر دید مستقیم Line of Sight (LOS)

خط مستقیم از شیئی در معرض دید (فرستنده) تا چشم بیننده (گیرنده) را LOS تعریف می کنیم . این تعریف که برای نور ارائه شده است ، برای RF نیز می تواند استفاده شود ؛ به این دلیل که امواج رادیویی نیز در خط مستقیم حرکت کرده ، مثل نور دچار انعکاس و خمیدگی می شوند .

Line of Sight

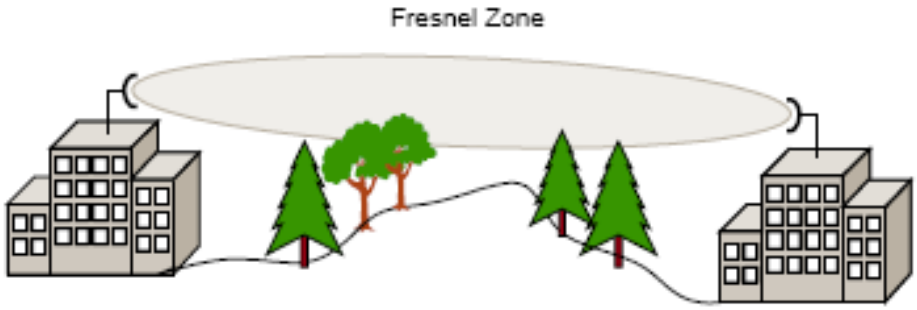


Cisco in Persian

منطقه فرزنل Fresnel Zone

یکی از مسایل مهمی که در طراحی و یا حل مشکل RF باید در نظر داشت Fresnel Zone است. این ناحیه در واقع محیطی است پیرامون LOS ، که به شکل یک سری بیضی متحدالمرکز دو نقطه در RF را بهم متصل می کند . اگر مانعی در این محیط قرار گیرد ، روی ارتباط ما تاثیر می گذارد . در پاره ای از مواقع موجب از بین رفتن ارتباط و یا ممکن است موجب Loss شود.

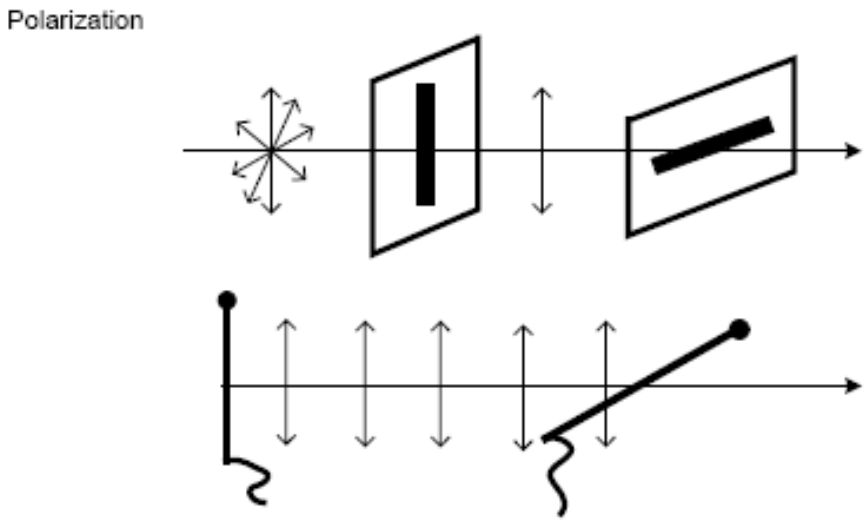
Fresnel Zone



در طراحی Fresnel Zone باید در نظر داشت که اگر حدودا ۲۰ تا ۴۰ درصد دارای مانع باشد مشکل زیادی را ایجاد نمی کند ، اما در صورتیکه موانعی مثل درخت (که دارای رشد است) وجود داشته باشد ، بهتر Fresnel Zone بدون مانع و با حدود صفر درصد مزاحمت دید برقرار شود .

Polarization

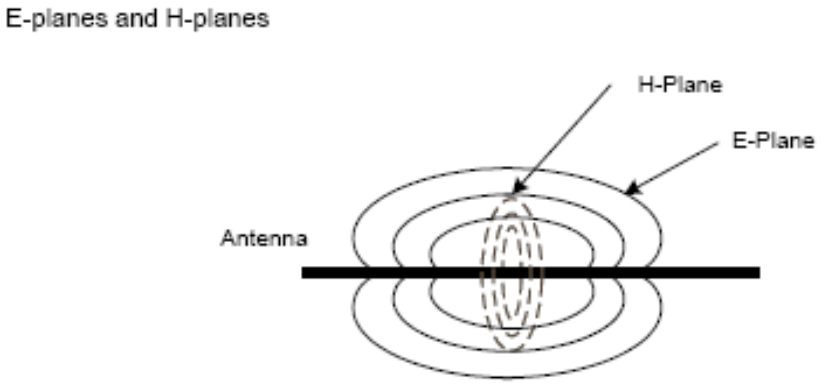
امواج رادیویی خواص الکترومغناطیسی دارند و از دو بخش الکتریکی و مغناطیسی تشکیل شده اند . در واقع ما با موج الکتریکی و جهت و موقعیت این موج نسبت به زمین ، Polarization را تعریف می کنیم .



امواج حاصل از یک آنتن به موازات آن منتشر می شوند ؛ در نتیجه امواج یک آنتن Vertical (عمودی) ، دارای Polarization عمودی خواهند بود (زیرا توسط یک قطعه فلزی روی آنتن و موازی با آن منتشر می شوند) ، و اگر آنتن گیرنده نیز به همان گونه Polarize نشده باشد ، دچار مشکل در دریافت خواهد شد .

Cisco in Persian

آنتن های AP ها بصورت عمود بر زمین و Vertical هستند و آنتن های کارت های PCMCIA بسختی دارای پوشش مناسب و کافی هستند . به همین دلیل ، تغییر مکان Laptop ها در آنتن دهی بهتر آنها نقش زیادی دارد . این در حالیست که کارتهای نصب شده روی PDA ها (بدلیل Vertical بودن موقعیت PCMCIA) و همچنین آنتنهای داخل Laptop ها (که اکثرا کنار مانیتور هستند) ، بهتر عمل می کنند .

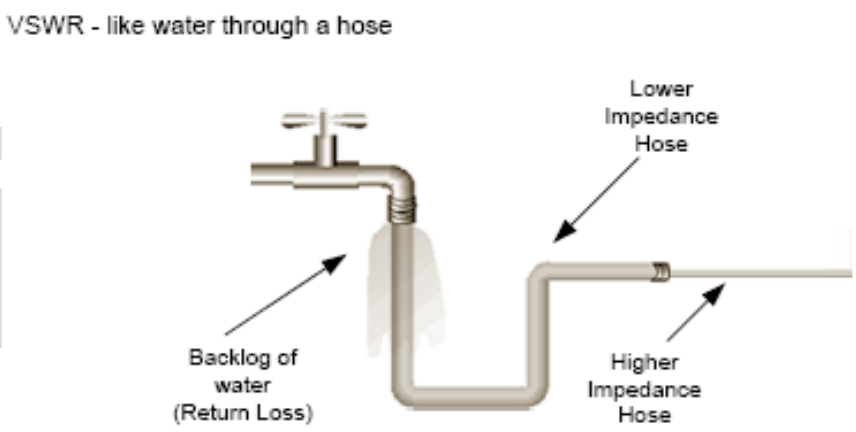


پیشنهاد می شود در جایی که تعداد PCMCIA ها زیاد است آنتن های AP ها را بصورت Horizontal (افقی) قرار دهیم.

Voltage Standing Wave Ratio (VSWR)

VSWR وقتی اتفاق می افتد که مقاومت بین دو دستگاه در یک سیستم RF غیرهمسان باشد. این اختلاف مقاومت ، موجب Return loss می شود که در اثر برگشت جریان در خلاف جهت فرستنده (transmitter) ، مقداری از Power هدر می رود و به آنتن نمی رسد . علامت شناسایی این مشکل ، اختلاف سطح سیگنال (Signal Level) است (یعنی بجای آنکه ثابت بماند ، متغیر می شود).

میزان VSWR یک نسبت است و اغلب به صورت ۱:۱/۵ است؛ که عدد دوم همیشه ۱ می باشد (زیرا که مقدار اصلی است و عدد اول متناسب با آن مشخص می گردد). هر چه عدد سمت راست به یک نزدیکتر باشد ، بهتر است . VSWR را بوسیله SWR Meter میتوان اندازه گرفت. آب و رطوبتی که به داخل کابل و کانکتور ها نفوذ می کند ، در خوشبینانه ترین حالت ، موجب افزایش VSWR می شود؛ از همین رو دستگاه های Outdoor باید به بهترین شکل محافظت و درزگیری شوند .



مثال کاربردی در مورد آنتن ها

می خواهیم در طبقه ای از یک بیمارستان با یک راهروی بلند و اتاق های مشرف به آن، یک WLAN طراحی کنیم ، در حالیکه سیگنال به طبقه فوقانی و تحتانی نیز برسد.

در این مثال می توانیم بجای این که از چندین AP با آنتن های Omni-Directional استفاده کنیم ، از آنتن Patch که Semi-Directional هستند بهره برده و آنرا در انتهای راهرو قرار دهیم . برای پوشش بهتر اتاق های دو طرف راهرو ، به آنتن با Gain بالا نیاز داریم که با توجه به کوچک شدن Vertical Beamwidth و ضعیف شدن سیگنال در جهت عمودی ، از آن صرف نظر کرده و از یک Patch دیگر در انتهای دیگر راهرو استفاده می کنیم . بدین ترتیب علاوه بر پوشش عمودی (طبقات بالا و پایین) ، راهرو و اتاق ها (افقی) را نیز پوشش داده و در هزینه نیز صرفه جویی کرده ایم .

Cisco in Persian

نکته : قانون 6 dB می گوید بازای افزایش EIRP به میزان 6dB ، دو برابر به مسافت پوشش افزوده می شود و بالعکس . این قانون به Path Loss (در واقع Free Space Path Loss) اشاره می کند .

دستگاه های جانبی Wireless

در این بخش، با انواع تجهیزات و دستگاههای جانبی پرکاربرد در شبکه های وایرلس آشنا می شویم .

✓ RF Amplifier

- **Unidirectional**: تقویت سیگنال قبل از ارسال توسط آنتن.
- **Bidirectional**: تقویت حساسیت گیرنده آنتن قبل از AP، پس از دریافت.

A sample of a fixed-gain RF amplifier

RF amplifier placement in the wireless LAN system

RF Attenuator ✓

می تواند در ورودی یا خروجی RF قرار گیرد. Attenuator و Amplifier هر یک به دو صورتFixed و Variable موجود می باشند که توسط تنظیم کردن نوع Variable آنرا میتوان به میزان مختلف تقویت و یا تضعیف کرد. استفاده از Attenuator های Variable پیشنهاد نمی شود.

A sample of a fixed-loss RF attenuator

A sample of a RF step attenuator (variable loss)

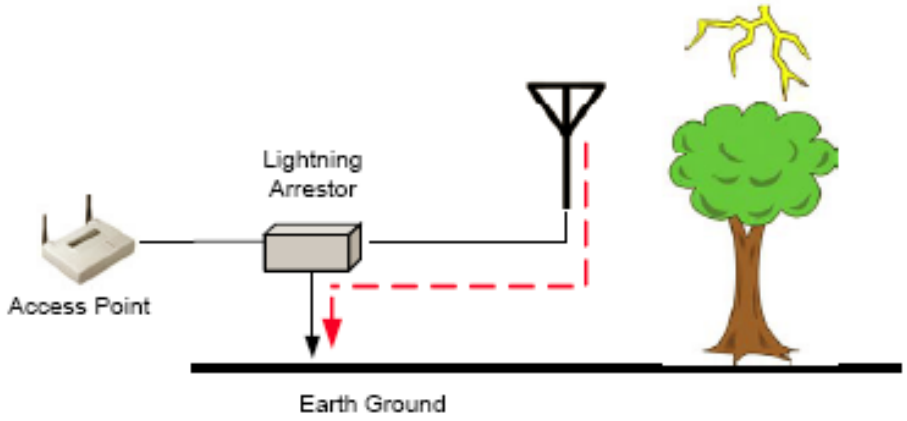
Cisco in Persian

Lightning Arrestor ✓

جریان ناپایدار و زودگذر رعد و برق (به اجسام نزدیک به محل)، انرژی الکتریکی زیادی را به زمین منتقل می کند . از آنجا که کابل Coax بسیار مستعد نسبت تحت تاثیرقرارگرفتن ازجریان محیط است و موجب بروز مشکل و انتقال جریان شدید به AP و Bridge می شود ، از Lightning Arrestor استفاده می کنیم . این Arrestor ، بر خلاف گمان همگان برای تضیف برخورد آذرخش به سیستم نیست و توان چنین مقاومتی را مسلما ندارد ، بلکه پس از برخورد آذرخش به جسم نزدیک و ایجاد جریان فراگذر در Line Transmission ، سیستم آنرا تشخیص داده و به سرعت گازی که در داخل خود قرار دارد را Ionize (تجزیه به یون) می کند و ارتباطی با مقاومت کم با زمین برقرار می کند .

Sample lightning arrestors

A lightning arrestor installed on a network



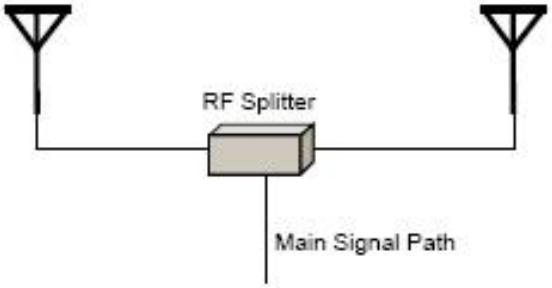
RF Splitters ✓

این دستگاه ، سیگنال RF را از یک ورودی به دو یا چند خروجی یکسان منتقل می کند که برای استفاده دو آنتن و یا برای اندازه گیری Power و اتصال آنتن همزمان مورد استفاده قرار می گیرد .

Cisco in Persian

Sample RF Splitters

A RF Splitter installed on a network



RF Connector ✓

انواع و اقسام Connector برای شبکه بی سیم مورد استفاده بوده است که طبق قوانین FCC هر سازنده Connector مختص به خود را استفاده می کند ؛ بطور مثال دو گونه N Connector و SMA را می توان نام برد .

Sample N-type and SMA connectors

The N Connector The SMA Connector

RF Cable ✓

کابل شبکه RF هر چه کوتاه تر، کم Loss تر و از قبل Connector زده شده (نه دست ساز) باشد بهتر است . از انواع معروف آن Andrew (Heliax)، Belden (RF) و Times Microwave (LMR) هستند .

کابل های رابط connector استاندارد به دستگاه سازنده را Pigtail می گوییم.

Coaxial cable attenuation ratings (in dB/foot at X MHz)

LMR CABLE	30	50	150	220	450	900	1500	1800	2000	2500
100A	3.9	5.1	8.9	10.9	15.8	22.8	30.1	33.2	35.2	39.8
195	2.0	2.6	4.4	5.4	7.8	11.1	14.5	16.0	16.9	19.0
200	1.8	2.3	4.0	4.8	7.0	9.9	12.9	14.2	15.0	16.9
240	1.3	1.7	3.0	3.7	5.3	7.6	9.9	10.9	11.5	12.9
300	1.1	1.4	2.4	2.9	4.2	6.1	7.9	8.7	9.2	10.4
400	0.7	0.9	1.5	1.9	2.7	3.9	5.1	5.7	6.0	6.8
400UF	0.8	1.1	1.7	2.2	3.1	4.5	5.9	6.6	6.9	7.8
500	0.54	.70	1.2	1.5	2.2	3.1	4.1	4.6	4.8	5.5
600	0.42	.55	1.0	1.2	1.7	2.5	3.3	3.7	3.9	4.4
600UF	0.48	.63	1.15	1.4	2.0	2.9	3.8	4.3	4.5	5.1
900	0.29	0.37	0.66	0.80	1.17	1.70	2.24	2.48	2.63	2.98
1200	0.21	0.27	0.48	0.59	0.89	1.3	1.7	1.9	2.0	2.3
1700	0.15	0.19	0.35	0.43	0.63	0.94	1.3	1.4	1.5	1.7

Cisco in Persian

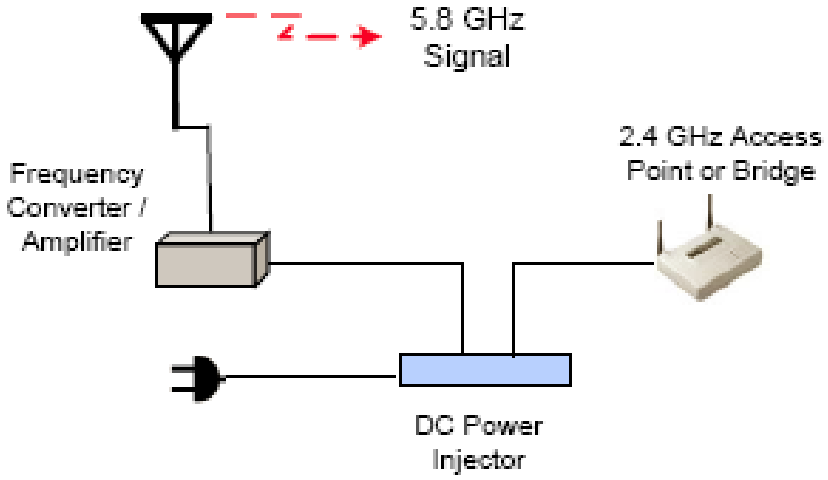
Frequency Converter ✓

مبدل فرکانس برای منطقه ای که اجازه استفاده از فرکانس خاصی به ما داده نمی شود (ترافیک فرکانسی) بسیار کارآمد است و بهتر از تغییر کل سیستم Wireless می باشد . پس از تبدیل ، مسلما باید از آنتن و کابل مرتبط با خروجی استفاده کرد . بطور مثال : 2.4 to 5.8 GHz Frequency Converter.

Sample frequency converter

Cisco in Persian

Using a frequency converter



✓ Test Kits

از Signal Generator و Power Meter برای تست کابل، کانکتور و ... می توان بهره برد .

Sample test kit

Cisco in Persian

✓ Power over Ethernet (PoE)

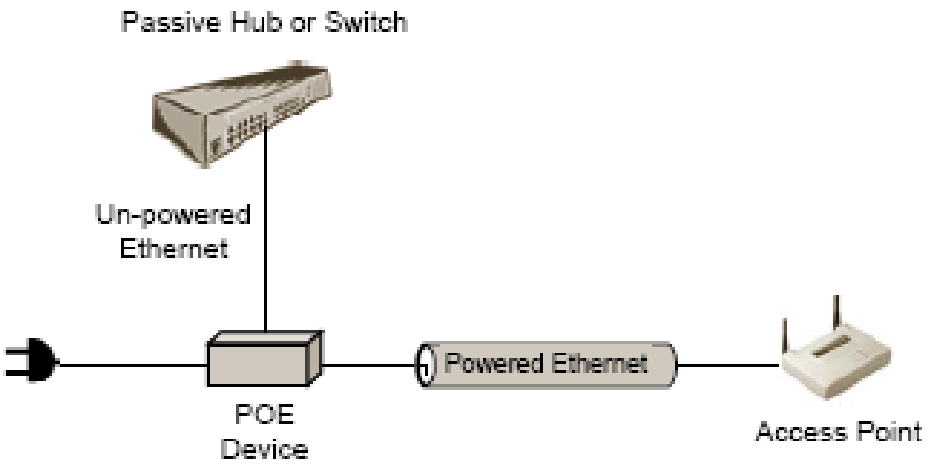
PoE ، روش ارائه برق DC روی کابل CAT 5 به AP است. در واقع کابل علاوه بر انتقال Data ، برق را نیز منتقل می کند . PoE در سه نوع و گونه مختلف قابل استفاده است:

- Single-port DC voltage injectors
- Multi-port DC voltage injectors
- Ethernet switches with PoE

در ضمن هیچ استاندارد رسمی برای PoE وجود ندارد و سازندگان از استاندارد های خود برای ارایه PoE استفاده می کنند . هرچند ، IEEE در حال ارائه استاندارد 802.3af برای این کار است. (در حال حاضر استاندارد شده – این مطلب قدیمی است!!!)

برای دستگاه هایی که PoE را پشتیبانی نمی کنند ، می توان از Picker یا Tap استفاده کرد (که به کابل متصل شده و جریان DC را مستقلا به یک Jack منتقل می کند و به دستگاه می دهد ، در واقع می توان گفت که Picker یک Ethernet Splitter است.)

PoE installation



Cisco in Persian

A single-port PoE injector

فصل چهارم : سازمان ها و استانداردهای وایرلس

- ❖ استانداردها و سازمان ها
- ❖ باندهای فرکانسی آزاد طبق قوانین FCC
  - ✓ باند فرکانسی ISM
  - ✓ باند فرکانسی UNII
- ❖ قوانین میزان توان (FCC)
  - ✓ Point to Multi-point
  - ✓ Point to Point
- ❖ استانداردهای IEEE در مقابل ETSI
- ❖ استانداردهای IEEE 802.11
  - ✓ 802.11
  - ✓ 802.11b
  - ✓ 802.11a
  - ✓ 802.11g
  - ✓ 802.11h
- ❖ استاندارد IEEE 802.11i
- ❖ استاندارد IEEE 802.16
- ❖ سایر ارتباطات بیسیم (رقبای 802.11)
  - ✓ OpenAir
  - ✓ Home RF
  - ✓ Bluetooth
  - ✓ IrDA

Cisco in Persian

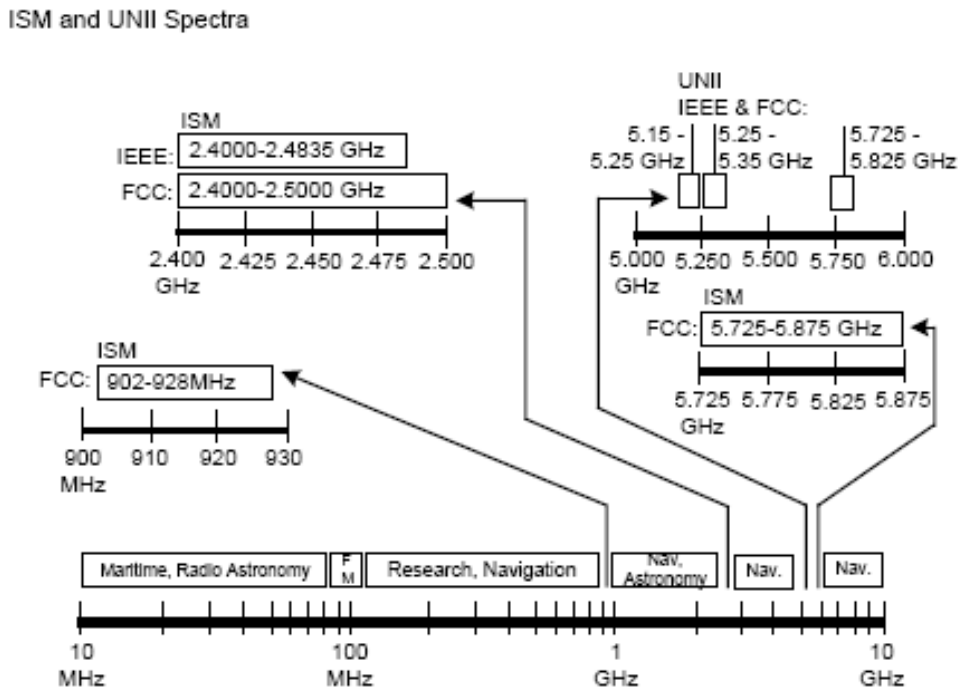
استاندارد ها و سازمان ها

از آنجا که Wireless LAN از فرکانسهای رادیویی جهت ارتباط بهره می برد ، قوانین و مقرراتی نظیر رادیو AM/FM را شامل می شود. Federal Communication Commission (FCC) تنظیم کننده قوانین استفاده از Wireless LAN است و کلیه ی قوانین مخابرات بی سیم در آمریکا توسط FCC وضع می شود .

IEEE در آمریکا و ETSI (European Telecommunications Standard Institute) در اروپا به وضع استاندارد های ارتباطات می پردازد.

باندهای فرکانسی آزاد طبق قوانین FCC

- **باند فرکانسی ISM (Industrial – Scientific – Medical)**



ISM Band فرکانسهای قابل استفاده بصورت License Free (بدون نیاز به اخذ مجوز) است که توسط FCC از پیش برای مصارف صنعتی، علمی و درمانی رزرو شده است.

مصارف	طول	فرکانس
Cordless Phone, Wireless Cam, WLAN	26 MHz	902-928 MHz
IEEE 802.11, IEEE 802.11b, IEEE 802.11g	100 MHz	2.4-2.5 GHz
مربوط به WLAN نیست	150 MHz	5.72-5.87 GHz

باند فرکانسی UNII (Unlicensed National Information Infrastructure)

از سه بازه فرکانسی 100 MHz، هرکدام ۴ کانال (4 Channels) تشکیل شده است.

مصارف	IEEE Power	طول	فرکانس
IEEE 802.11a Lower Band (indoor)	40 mW	100 MHz	5.15-5.25
IEEE 802.11a Middle Band (in/out)	200 mW	100 MHz	5.25-5.35
IEEE 802.11a Upper Band (outdoor)	800 mW	100 MHz	5.72-5.82

میزان Power مجاز FCC،25% بیشتر از میزان استاندارد IEEE است. یعنی به ترتیب 50mW، 250mW و 1W است.

قوانین میزان Power (FCC)

Point to Multi-Point

Max EIRP: 4W
Max Intentional Radiator: 1W

توجه : به ازای هر 6 dBi اضافه در EIRP ، باید از Intentional Radiator ، 3dB (از مجموع 30dBm) کم کنیم.

مثال:

Intentional Radiator=1W (30dBm) + 12dB Antenna -> EIRP=16W > 4W

–> 16 = 4 + 6 + 6 –> Intentional Radiator – 6dB (30 – 6) = 24dBm

–> EIRP = 24dBm (250mW) + 12dBi = 36dBm = 4W

Point to Point

Max EIRP: Unlimited

Max Intentional Radiator: 1W

اگر Gain آنتن را 6dB فرض کنیم ، به ازای هر 3dB که بیشتر باشد باید یک dB از Intentional Radiator کم کنیم. در ارتباط نقطه به نقطه ، FCC محدودیتی برای EIRP قایل نیست ؛ البته بشرطی که Gain آنتن موجب افزایش آن شود.

در باند UNII ، آنتن نیز به 23dBi محدود می شود (1W Intentional Radiator + 23dBi = 200W) که البته به ازای هر dB بیش از حد مجاز، می توانیم از Power بکاهیم.

Cisco in Persian

استاندارد های IEEE در مقابل European Telecom Standard Institute :

- Personal Area Network (PAN) IEEE 802.15 – ETSI HiperPAN
- Wireless LAN IEEE 802.11 – ETSI HiperLAN
- Wireless MAN IEEE 802.16 – ETSI HiperMAN – HiperAccess
- Wirelss WAN IEEE 802.20 – 3GPP – EDGE

سری استاندارد های IEEE 802.11

استاندارد 802.11

استاندارد اصلی Wireless LAN است که پایین ترین سرعت را درهر دو تکنولوژی RF و انتقال نوری شامل می شود و توسط IEEE در سال ۱۹۹۷ ارایه شد.

Cisco in Persian

استاندارد 802.11b

استانداردی سریعتر با حوزه ارسال محدودتر که اغلب آنرا با نام Wi-Fi می شناسند و این استاندارد در ۱۹۹۹ بعنوان اصلاحیه IEEE 802.11 شناخته شد.

استاندارد 802.11a

این استاندارد که بسیار سریعتر از 802.11b (اما ناسازگار با آن) است در سال ۱۹۹۹ توسط IEEE معرفی شد. این استاندارد از فرکانس 5GHz باند UNII استفاده می کند و بهمین دلیل با استاندارد های 802.11 دیگر سازگار نیست . با سرعتهای 6, 9, 12, 18, 24, 36, 48 & 54 Mbps کار می کند و با استفاده از Rate Doubling به 108 Mbps نیز دست یافته است . هرچند که در IEEE 802.11a فقط به ۶، ۱۲ و 24Mbps اشاره شده است .

این استاندارد از تکنولوژی OFDM (Orthogonal Frequency Division Multiplexing) استفاده می کند و در واقع عامل موفقیت در سرعت این استاندارد است . (802.11g نیز که بعدا ارائه شد از این تکنولوژی جهت دستیابی به 54Mbps سود می برد.)

در این استاندارد برای استفاده In-door ، چهار کانال Lower Band و چهار کانال Middle Band (طبق UNII) داریم که در کانال 20 MHz پهنا دارد .

OFDM هر کانال (20 MHz) را به 52 Sub-carrier تقسیم می کند که هر یک 300 KHz پهنا داشته و همزمان از تمام این کانال ها برای ارسال بصورت موازی بهره می برد و بخاطر احتمال وقوع خطا از FEC استفاده می کند .

Forward Error Correction که به 802.11a اضافه شد ، با استفاده از تکثیر یک کپی دیگر ازاطلاعات (که Primary Data توسط یک الگوریتم از Secondary Data قابل استنباط است) وقوع خطا را به حداقل می رساند.

استاندارد 802.11g

آخرین استاندارد ارائه شده بر پایه 802.11 که سرعت بالایی نظیر 802.11a و سازگاری مناسبی با 802.11b دارد ، تا Upgrade های 802.11b را ارزانتر سازد و در سال ۲۰۰۳ ارائه شده است . از OFDM بهره می برد و برای سازگاری با استاندارد های پیشین DQPSK را نیز پشتیبانی می کند.

استاندارد 802.11h

برای سازگاری با ETSI Hiper-Lan 2 که مشابه 802.11a است ، توسط IEEE ارائه شده است.

Cisco in Persian

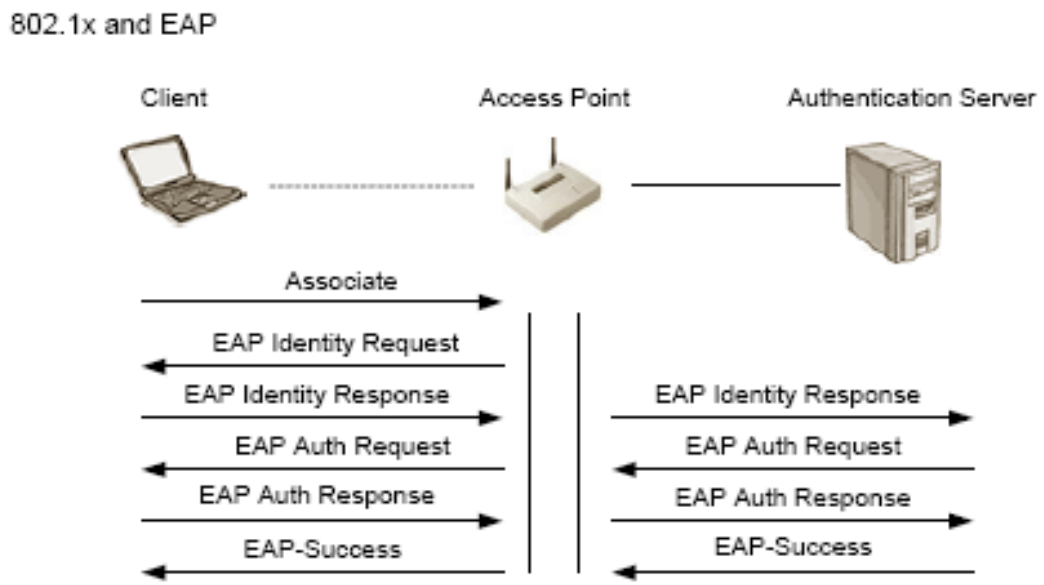
استاندارد 802.11n در زمان نگارش مقاله مصوب نشده بود که به سرعت ۳۰۰ مگابیت در ثانیه میرسد و بکمک MIMO پوشش بهتری را بکمک سه آنتن بهمراه دارد.

استاندارد IEEE 802.11i

استاندارد IEEE 802.11i، شامل موارد امنیتی ذکر نشده در ۸۰۲,۱۱ است که شامل 802.1x ، EAP ، AAA ، Key Generation و Mutual Authentication است . برای بالابردن امنیت شبکه بی سیم راه حل استفاده از 802.1x ، VPN و EAP است .

802.1x دستیابی به لایه دو را تنها پس از Authentication میسر می سازد . اجزای 802.1x عبارتند از :

- Supplicant (Client)
- Authenticator (AP)
- Authentication Server (RADIUS)



EAP در LAN مشابه CHAP و PAP در PPP است . در ادامه بحث ، انواع EAP را تشریح میکنیم:

- EAP-MD5
- EAP-LEAP
- EAP-TLS
- EAP-TTLS
- EAP-PEAP
- EAP-SRP
- EAP-SIM

حال به بررسی هر یک می پردازیم:

- MD5 از اولین نمونه های اجرایی EAP است که از MD5 استفاده کرده است.

- LEAP (Lightweight) نمونه EAP بکارگرفته شده در دستگاههای سیسکو است و قابلیتهای امنیتی زیادی نظیر Dynamic WEP Generation را داراست.

- TLS (Transport Layer Security) با استفاده از Mutual Authentication و Certificate بین کاربر و سرور عمل کرده و از Dynamic User & Session-based WEP key استفاده می کند که در ویندوز نیز پشتیبانی می شود.

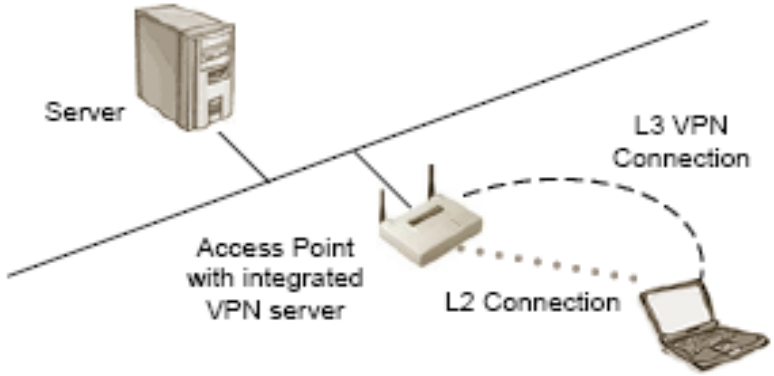
- TTLS (Tunneled Transport Layer Security) بر اساس EAP-TLS ساخته شده که علاوه بر مزایای آن تنها به Server-side Certificate نیاز است . در واقع مراحل Authentication نیز داخل یک تونل TLS پنهان می شوند . این روش توسط Funk Software و Certicom ارائه شده است .

- PEAP (Protected) توسط سیسکو و مایکروسافت در رقابت با TTLS ارائه شده که علاوه بر مزایای آن ، در نسخ Windows XP SP1 و Cisco ACU 5 به بعد نیز Built-in پشتیبانی می شود.
- SRP (Secure Remote Password) یک پروتکل امن برای مواردی است که کاربر تنها نیاز به خاطر سپردن یک رمز کوچک را دارد.

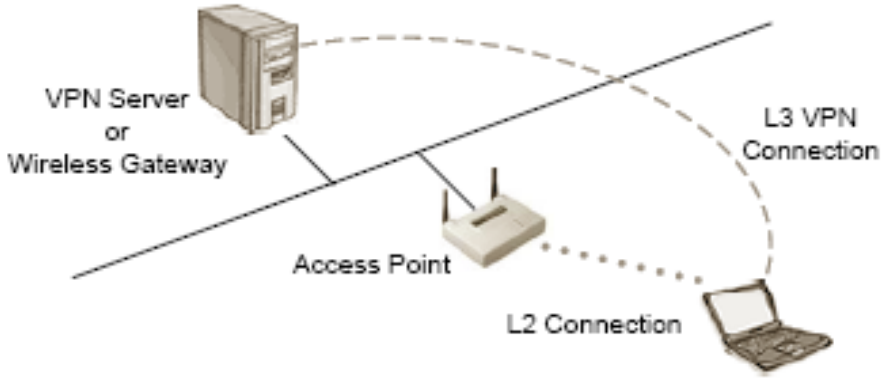
- SIM (GSM Subscriber Identity Module) برای ارتباطات Mobile IP و قابلیت Authentication کاربر با استفاده از اطلاعات SIM Card آن در شبکه موبایل است. این ایده برای استفاده از خطوط موبایل در ارتباط شبکه ی بی سیم نیست ، بلکه استفاده از آن برای شناسایی کاربر است.

Cisco in Persian

Access point with an integrated VPN server



Access point with an external VPN server



استاندارد 802.16

این استاندارد ، خود به چندین استاندارد دیگر تقسیم می شود، از جمله :

- IEEE 802.16
- IEEE 802.16a
- IEEE 802.16e

نکته : عامل موفقیت این تکنولوژی استفاده از QAM و QPSK است که در 3G نیز بکار گرفته شده اند . فرکانس های زیر 10GHz قادرند از موانع عبور کنند ؛ از این رو سیستم های GSM از 900MHz تا 1800MHz استفاده می کنند.

نکته : WiMAX یا Worldwide Interoperability for Microwave Access سازمانی برای تطابق بین محصولات سازندگان در رابطه با ۸۰۲,۱۶ است (مثل WiFi و ۸۰۲,۱۱) .

دیگر ارتباطات بی سیم (رقبای 802.11)

در این بخش ، با سایر استانداردهای بی سیم که برای مصارف مشابه استفاده می شوند ، آشنا می شویم .

Cisco in Persian

استاندارد OpenAir

این استاندارد توسط Wireless LAN Interoperability Forum (WLIF) وضع شده و از تکنولوژی FHSS با حداکثر سرعت 800Kbps تا 1.6Mbps استفاده می کرد . این استاندارد بعنوان یک جایگزین برای ۸۰۲,۱۱ در زمان خود مطرح بود ، اما با آن سازگار نبود .

استاندارد HomeRF

این استاندارد در باند 2.4 GHz کار می کند و در هر ثانیه ۵۰ بار Frequency Hopping انجام داده و بسیار سریع تر از ۸۰۲,۱۱ با FHSS همراه است.

HomeRF 2 از Wide Band Hopping بهره برده و به 10 Mbps دست پیدا کرد . در این تکنولوژی از SWAP (یا همان Shared Wireless Access Protocol که در واقع تلفیقی از CSMA و TDMA (ارتباطات موبایل) است و خود ادغامی از استاندارد های DECT و ۸۰۲,۱۱ بوده است) استفاده شده و دارای خصوصیت WEP (امن تر از 802.11 WEP) و سازگاری با استاندارد قدیمی OpenAir است .

استاندارد Bluetooth

این تکنولوژی نیز از Frequency Hopping بهره برده و در هر ثانیه ۱۶۰۰ بار فرکانس خود را تغییر می دهد . Dwell time آن در حدود ۶۲۵ میکرو ثانیه است و در باند 2.4 GHz ISM ارتباط برقرار می کند . در عمل ، Bluetooth روی ۸۰۲,۱۱ ایجاد مشکل کرده و بعنوان All-band Noise شناخته می شود ؛ هر چند که خودش بخاطر مکانیزم Hopping دچار مشکل نمی شود . از این رو ، در مناطق WLAN ، پلاکارد های NO Bluetooth به چشم می خورد .

استاندارد ۸۰۲,۱۵ بنام Personal Area Network توسط IEEE برای Bluetooth ارایه شده است.

تجهیزات Bluetooth در سه کلاس Power دسته بندی می شوند: 1mW, 2.5mW, 100mW که کلاس دوم آنها 2.5mW برد ۱۰ متری دارد.

آدرس وب Bluetooth Special Interest Group (SIG):

www.bluetooth.com

Infrared Data Association (IrDA)

IrDA یک استاندارد نیست ، بلکه نام یک سازمان با مجموعه ای از استاندارد هاست که از ۱۹۹۳ شروع بکار کرده است . استفاده از مادون قرمز در ماشین حساب ها ، چاپگر ها و گوشی های همراه بسیار مرسوم است .

مادون قرمز تکنولوژی ای است که از نور استفاده می کند (بر خلاف Spread Spectrum که از RF بهره می برد) و در فواصل نزدیک حداکثر به 4Mbps دست می یابد که البته سرعت معمول آن 115 Kbps است و برای مصارف IR مناسب بنظر می آید.

از آنجایی که IrDA از نور استفاده می کند ، با شبکه های رادیویی هیچ تداخلی ندارد ؛ اما منابع نوری دیگر روی آن تاثیر می گذارند ، بطوریکه لینک های Point to Point مادون قرمز برد کم یک کیلومتری دارند و در روزهای آفتابی حتی ضعیف تر عمل می کنند (با توجه به اینکه نور خورشید ۶۰ درصد مادون قرمز است). همچنین از دیوارها عبور نکرده بلکه منعکس می شود . در مصارف In-door به آن Single Room Networking می گویند . همچنین نکته ی دیگر اینکه Power آن کم بوده و روی برد تاثیر گذار است (2 mW).

نکته ی قابل توجه اینست که IrDA از لحاظ امنیت بسیار قابل اطمینان است و در واقع می توان گفت که دارای شنود غیر ممکن است (no eavesdropping).

Cisco in Persian

فصل پنجم : شبکه های وایرلس و تکنیک های Spread Spectrum

Cisco in Persian

- مدولاسیون
- Spread Spectrum
  - FHSS ✓
  - DSSS ✓

Modulation

مدولاسیون ، یعنی تغییر سیگنال جهت استفاده در محیطی دیگر(مثل Modem که Digital را به Analog تبدیل می کند). در مدولاسیون از امواج electro-magnetic با سرعت بالا به عنوان Carrier (حامل) بهره می بریم ؛ سه تکنیک اصلی وجود دارد:

- ASKتغییر در دامنه
- FSK تغییر در فرکانس
- PSK تغییر فاز

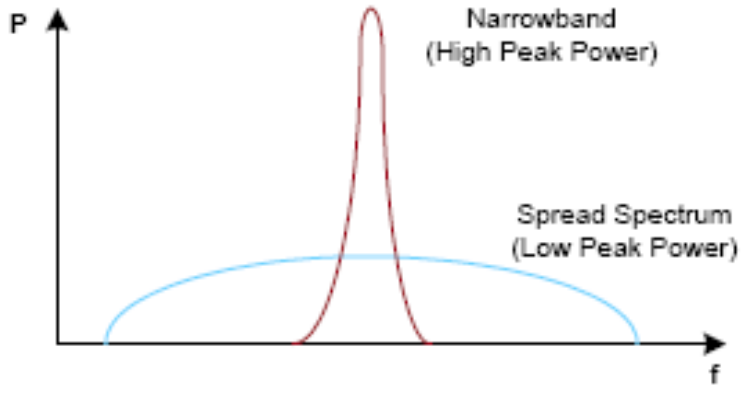
تکنیک Spread Spectrum

فن آوری Spread Spectrum همانند اغلب تکنولوژی های شبکه ، توسط ارتش برای اولین بار بکار گرفته شد و طی زمان و کاهش قیمت جهت اتصال شبکه های ساختمانها ، شرکتها و حتی ها استفاده در منازل ، همگانی شد .

تکنیک ارتباطی Spread Spectrum پس از Narrow Band برای استفاده ارتش ابداع شد و از پهنای باند پهن تری نسبت به آن بهره می برد ؛ در حالیکه Narrow Band دارای High-Peak Power و Power بالا برای ایجاد موج باریک (با پیک بالا) است و Jamming و اختلال براحتی در این سیستم ها صورت می گیرد . اما در Spread Spectrum که خود Noise گونه است و به سختی شناسایی می شود ، دقیقا عکس این قضیه صادق است .

Cisco in Persian

Narrow band vs. spread spectrum on a frequency domain



در زیر ، تفاوت Spread Spectrum و Narrowband را در میزان قدرت مصرفی می بینیم :

1 MHz Narrowband = 10 W Power
20 MHz Spread Spectrum = 100mW Power

عموما هر چه فرکانس کوچکتر باشد به Power بیشتر نیاز داریم.

FCC دو نوع کاربرد Spread Spectrum را برای استفاده در ارتباطات شبکه های بی سیم تنظیم کرده است که شامل FHSS و DSSS می شود.

FHSS (Frequency Hopping Spread Spectrum)

از 79 MHz فرکانس بین ۲,۴۰۲ تا ۲,۴۸۲۵ بعنوان Channel استفاده می کند و در هر ثانیه ۵ بار فرکانس خود را تغییر می دهد.
(Bluetooth در هرثانیه ۱۶۰۰ بار و HomeRF در هرثانیه ۵۰ بار تغییر فرکانس می دهند.)

Dwell Time زمانی است که روی یک فرکانس ساکن بوده (حدود ۱۰۰ تا ۲۰۰ میلی ثانیه) و بعد به فرکانس بعدی Switch می کند ؛ بین Switch فرکانسی ، وقفه ای هست که به آن Hop Time می گویند (که در حد ۱۰۰ میکروثانیه است).

هر جا خواستیم Throughput را بالا ببریم ، باید dwell time طولانی تر داشته باشیم؛ مگر آنکه Interference و اختلال فرکانسی زیاد باشد.

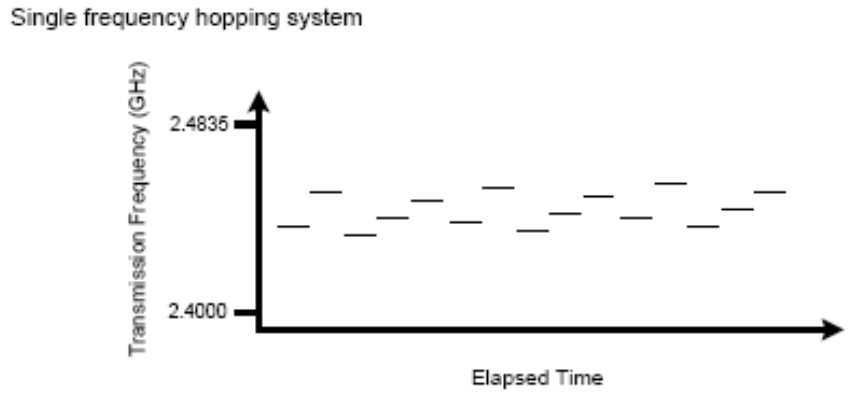
FCC میگوید بین دو Channel که پشت سرهم hopping دارند باید 6 MHz فاصله باشد و بعد از Hop های بعدی می توانیم از این Hop ها که جا انداختیم ، دوباره استفاده کنیم.

Cisco in Persian

دو قانون FCC داریم که می توان از یکی از آنها تبعیت کرد:

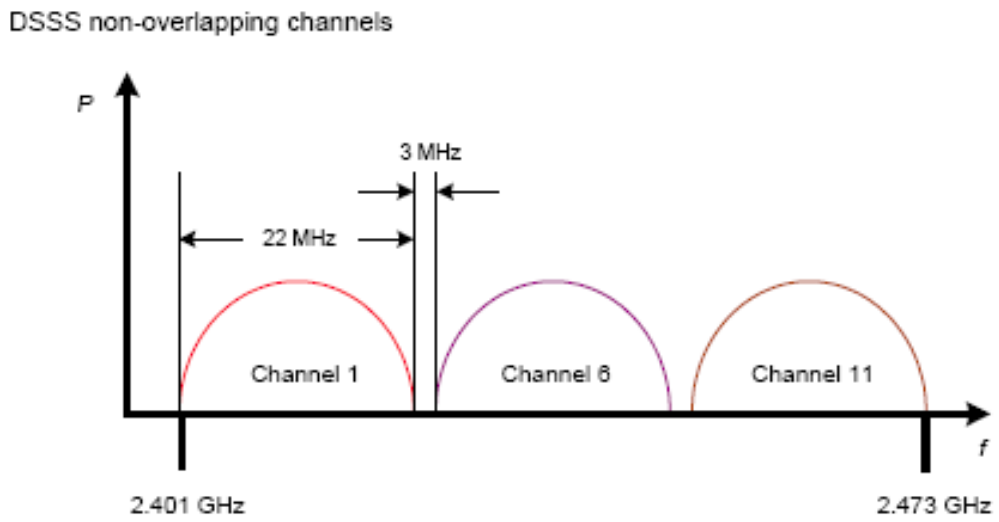
قانون اول می گوید حداقل باید ۷۵ فرکانس از ۷۹ فرکانس (هر کدام 1 MHz) را در یک دور استفاده کرد ؛ که بخاطر 1 MHz بودن Channel ها ، Intentional Radiator می تواند تا 1 W قدرت داشته باشد .

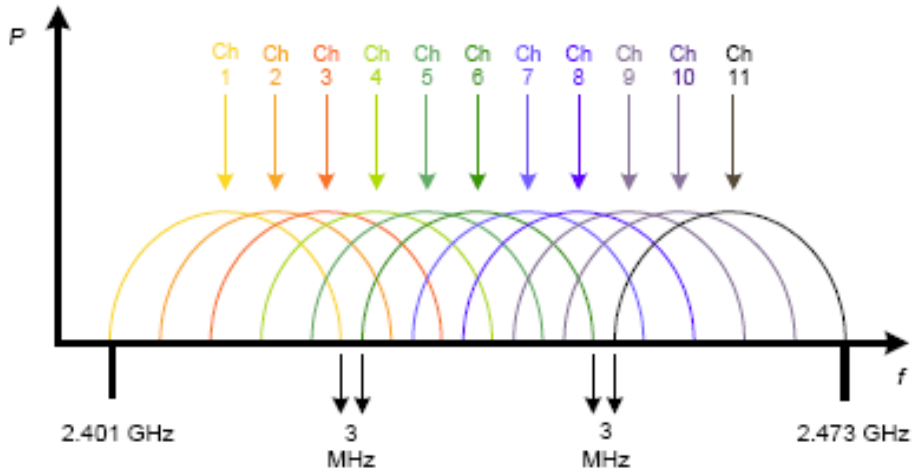
قانون دوم (مصوب ۲۰۰۰/۸/۳۱) می گوید شما حداقل از ۱۵ کانال 5 MHz با قدرت 125 mW می توانید بهره برید که مسلما با تغییر پهنای باند کانال قدرت مورد نیاز کاهش یافته است .



DSSS (Direct Sequence Spread Spectrum)

DSSS شامل ۱۱ کانال 22 MHz است که باهم همپوشانی دارند و تنها ۳ کانال (۱ و ۶ و ۱۱) با هم تداخل ندارند. DSSS نسبت به FHSS حساستر است (بخصوص تداخل با Narrowband) ، زیرا FHSS از 79 MHz در طول ارتباط استفاده می کند ، اما DSSS از 22 MHz.





DSSS بخاطر تنوع تولید کنندگانش و استقبال بازار ، از قیمتی بسیار ارزانتر از FHSS برخوردار است ، اما در یک مکان واحد (Co-location) ، تنها سه DSSS AP بدون تداخل کار می کنند ؛ هرچند FHSS به مراتب بیشتر، ولی تنها ۱ الی ۲ مگابیت Throughput دارد در حالیکه DSSS تا ۱۱ مگابیت خروجی مفید دارد.

هرچند بنظر می آید که FHSS امن تر است ، اما اینطور نیست ؛ چون تعداد تولید کنندگان آن انگشت شمار است و طبق استانداردهای از پیش تعیین شده ، Hoping انجام می دهد و براحتی Track می شود.

فصل ششم : ساختار شبکه ی 802.11

- ❖ SSID & Beacon
- ❖ Scanning
  - ✓ Passive Scanning
  - ✓ Active Scanning
- ❖ Association & Authorization
- ❖ Roaming
- ❖ توپولوژی های 802.11
  - ✓ BSS
  - ✓ ESS
  - ✓ IBSS

Cisco in Persian

SSID & Beacons

برای پیدا کردن Access Point ها و شبکه های بی سیم از SSID (Service Set ID) و Beacon استفاده می شود.

SSID نام شبکه است و یکتا (Unique)، از ۲ تا ۳۲ کاراکتر Case Sensitive . گاهی اوقات به آن ESSID نیز گفته می شود و این نام توسط Beacon ها ارسال می شود .

نکته قابل توجه این است که SSID (ESSID) بین AP ها و Client های شبکه باید دقیقا یکی باشد تا یک شبکه را تشکیل دهند و نباید با BSSID (Basic Service Set ID) اشتباه گرفته شود. (BSSID عددی HEX بطول ۶ بایت است که نشانگر AP است.)

Beacon Management Frame ها که به اختصار به آنها Beacon می گوییم ، فریم های کوتاهی هستند که از AP به Client ها ارسال می شود (البته در Ad hoc از client به client ارسال می گردند) تا ارتباط شبکه بی سیم را Synchronize(انطباق زمانی) کرده و سازمان دهند. از جمله وظایف Beacon ها می توان موارد زیر را عنوان کرد :

- **Time Synchronization :** برای تطبیق بازه های زمانی ارسال و دریافت بین AP و Client ها باید صورت بگیرد . بطور مثال زمان Hopping در FHSS را می توان نام برد . Beacon ها همچنین Beacon Interval را نیز مشخص می کنند تا بدانیم باید در چه زمانی منتظر Beacon بعدی باشیم.

- **FH/DS Parameters :** در واقع اطلاعات مربوط به Channel ها در DSSS و یا همچنین اطلاعات مربوط به Hop Sequence و Hop/Dwell time توسط Beacon ها اعلام می شوند .

- **SSID Information :** در Beacon ، SSID ارسال شده و Station با ملاحظه MAC Address فرستنده آن به شبکه ملحق می شود .

- **Traffic Indicator Map (TIM) :** برای مصرف کمتر باطری و Power ، Station ها به حالت Sleeping می روند ؛ اگر پیغامی برای آنها در Queue باشد ، اسم آنها در لیست ثبت می شود تا آنها مطلع شوند .

- **Supported Rates :** سرعت ها ی قابل پشتیبانی و پهنای باند مورد قبول AP را به همه اعلام می کند .

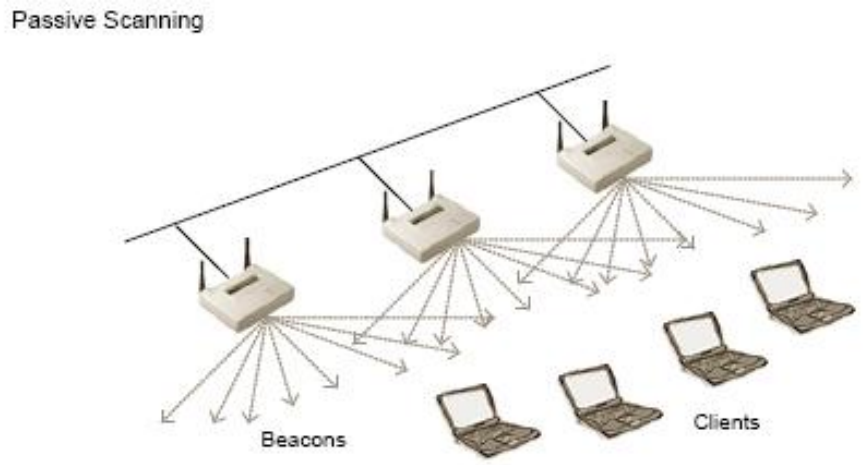
Cisco in Persian

Scanning

Client برای اتصال به شبکه بی سیم از طریق کارت PCMCIA یا USB خود ، به سیگنال ها گوش می دهد (Listen) تا شبکه ای را در محدوده برد خود پیدا کند . به این پروسه Scanning می گویند . Scanning به دو گونه صورت می گیرد : Active و Passive .

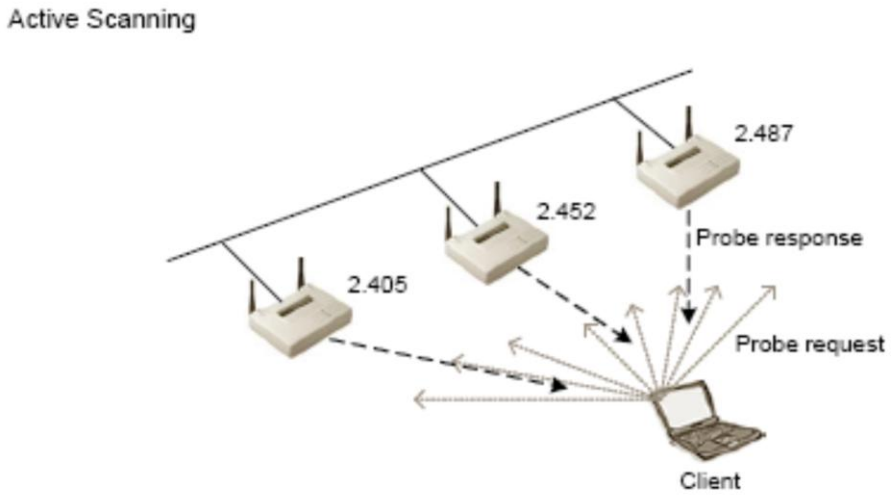
Passive Scanning

در این حالت Station بگوش می ایستد از AP، Beacon دریافت می کند و در صورت تمایل Join به شبکه می شود. SSID را روی Channel گرفته و Signal Strength نیز در هنگام دریافت مشخص می شود. Client حتی بعد از الحاق به شبکه نیز به Passive Scanning ادامه می دهد.



Active Scanning

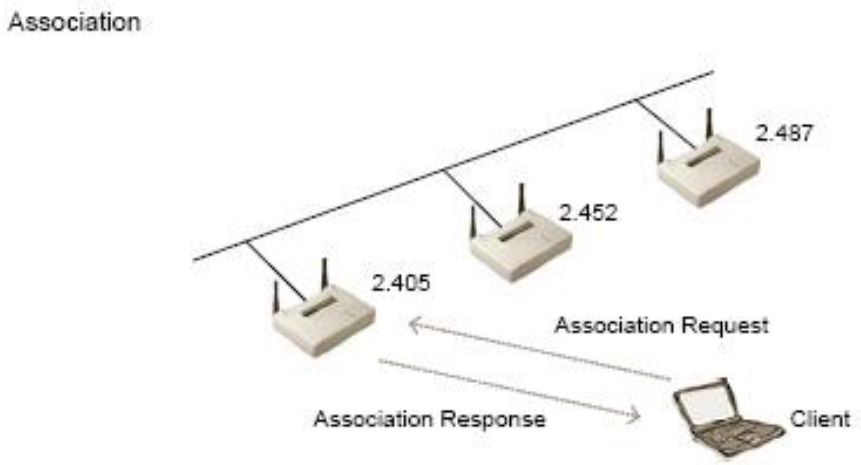
این وضعیت برعکس Passive عمل میکند و Client، SSID مورد نظر خود را اعلام کرده (Probe request) و منتظر جواب می ماند (Probe response) . در حالت دیگر Client یک SSID Broadcast میفرستد و هر APی که این Broadcast را دریافت می کند برای Client، SSID خود را می فرستند. (در صورت مجاز بودن از لحاظ امنیتی). این گونه جواب از طرف AP همانند Beacon است با این تفاوت که حاوی TIM و Timestamp نیست.



Association و Authentication

اولین گام در اتصال یک Station به شبکه بی سیم ، صدور مجوز برای اتصال از طرف AP (و یا یک RADIUS سرور) است . این Authentication بر اساس لایه دو و یک سری پارامترهای مربوطه است .

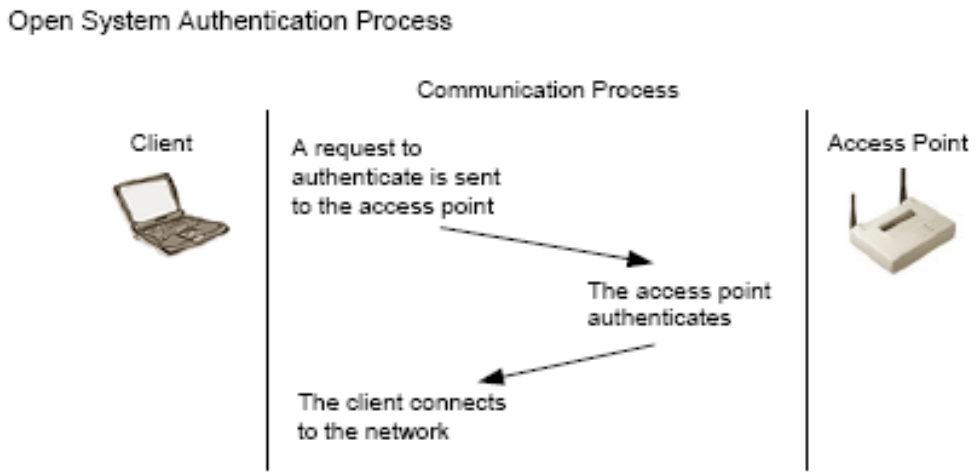
وقتی client مورد نظر Authenticate شد ، به AP مربوطه Associate می شود و پس از آن قادر به دریافت و ارسال در شبکه خواهد بود.



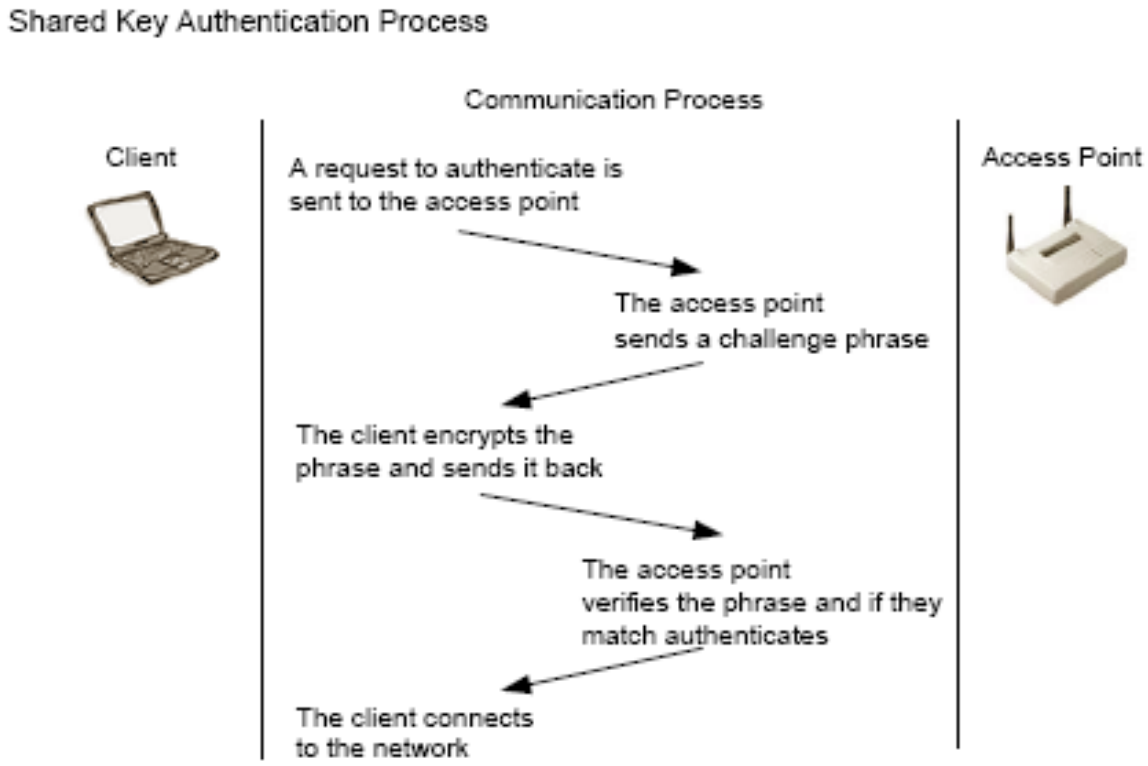
Cisco in Persian

استاندارد ۸۰۲,۱۱ دو گونه Authentication از قرار زیر را تعریف می کند :

- **Open System Authentication:** متد default است که در واقع تنها با دانستن SSID ، Client درخواست Authentication داده و AP در صورت قبول آنرا به شبکه متصل می کند . حتی اگر AP دارای تنظیمات WEP (برای رمزنگاری) باشد، در این مرحله از رمزنگاری استفاده نمی کند و پس از اتصال کامل و Association از آن بهره می برد . در این حالت تا زمانیکه Station به شبکه متصل نشده ، از رمزنگاری آگاه نمی شود .

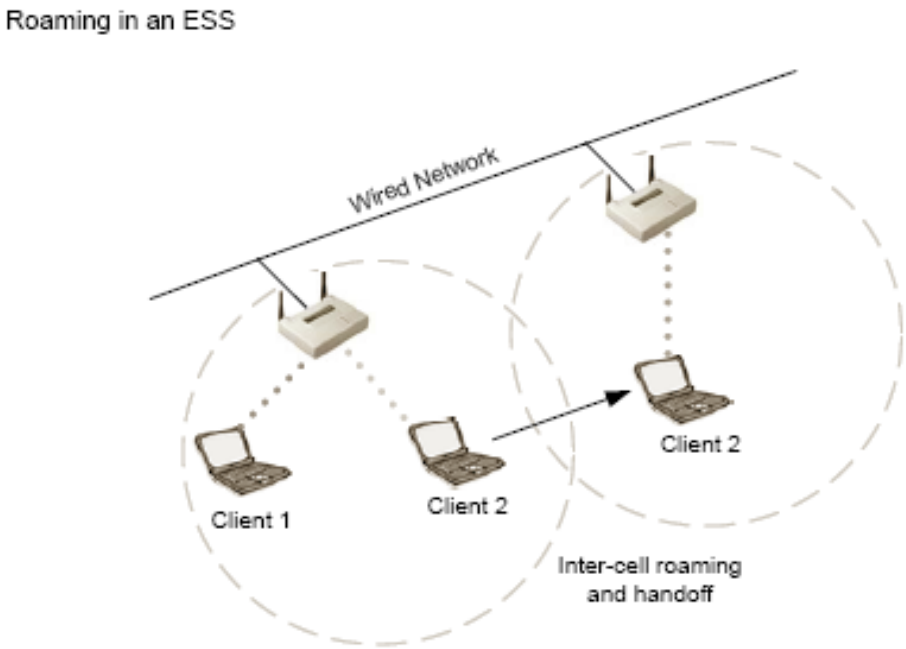


- **Shared Key Authentication**: در این روش از WEP در حین Authentication استفاده می شود . در واقع Client درخواست اتصال را به AP می فرستد ، AP یک Challenge بصورت Clear Text فرستاده تا Client با کلید WEP خود آنرا Encrypt کند و این جواب در سمت AP برای مجاز بودن اتصال Client چک می شود . این روش برای بالا بردن امنیت ارائه شده اما Hacker با نرم افزار خود ، متن Plain Text و Encrypted را گرفته و از روی آن ، می تواند کلید WEP را استنباط کند.



Roaming

Roaming را قابلیت انتقال و تحرک کاربر از یک Cell به Cell دیگر، بدون از دست دادن ارتباط تعریف می کنیم . برای دستیابی به این امتیاز ، شبکه باید دارای پوشش مناسب باشد . همچنین منطقه بین دو Cell باید در قسمتی دارای Overlap بوده تا امکان راهیابی از یک Cell به Cell دیگر وجود داشته باشد و ارتباط قطع نشود.



در ارتباط Packet based LAN ، عمل Roaming در حین Packet Switching صورت می گیرد . اما در ارتباط تلفنی ، بین یک مکالمه امکان Roaming وجود دارد . در ارتباط تلفنی ، سکوت یا قطعی لحظه ای کمتر ممکن است مکالمه را دشوار سازد ، اما در ارتباط Packet based تنها منجر به پایین آمدن Performance خواهد شد.

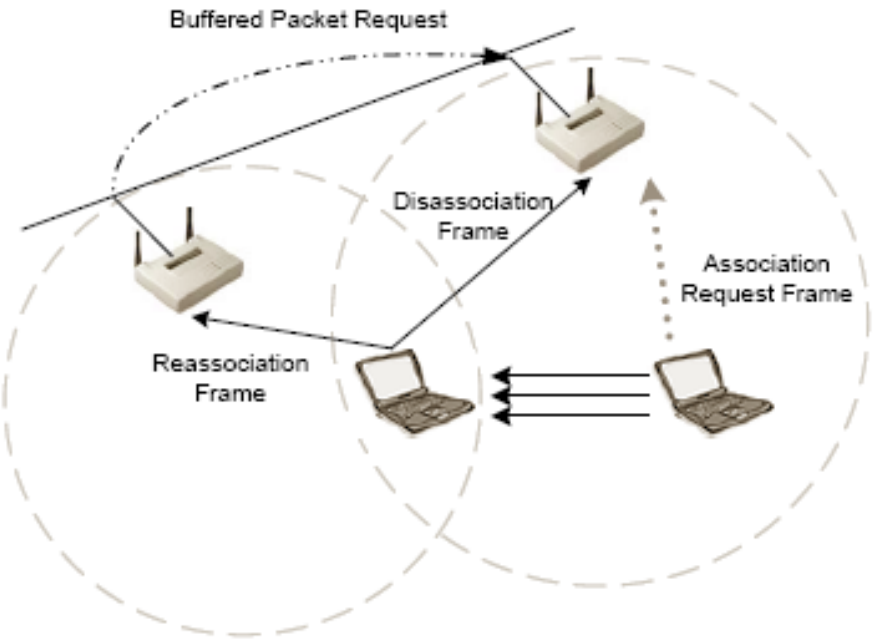
در استاندارد 802.11، Roaming بطور کامل و کاربردی تعریف و تشریح نشده است و تنها به Active/Passive Scan و Reassociation اشاره شده است.

در واقع Reassociation وقتی است که یک Station از یک AP به AP دیگر ، Associate می شود(به عبارتی دیگر ، عضو می گردد).

بر اساس Beacon های دریافتی ، Client می تواند قدرت (Strength) سیگنال AP را نسبت به خود ارزیابی کند .

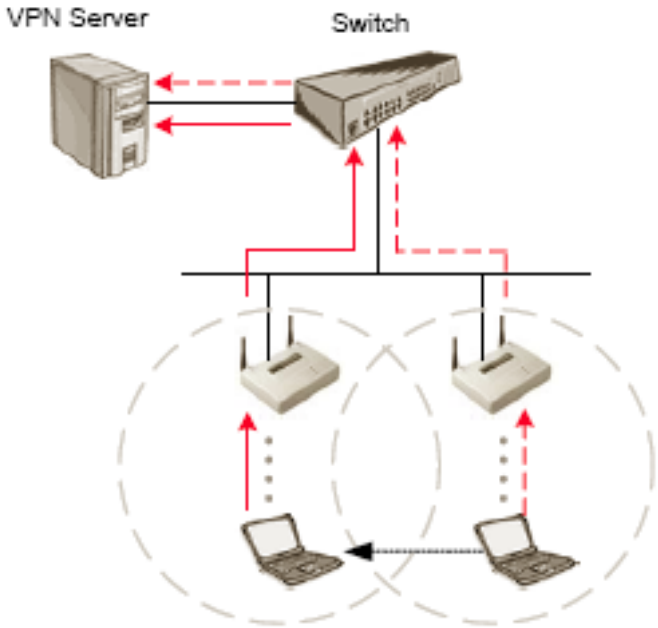
برای بکارگیری Roaming در شبکه بی سیم ، Mobile IP استاندارد IETF که در RFC 2002 ارائه شده ، از طریق بکارگیری Home Agent و Foreign Agent این مهم را فراهم می آورد .

Roaming with reassociation

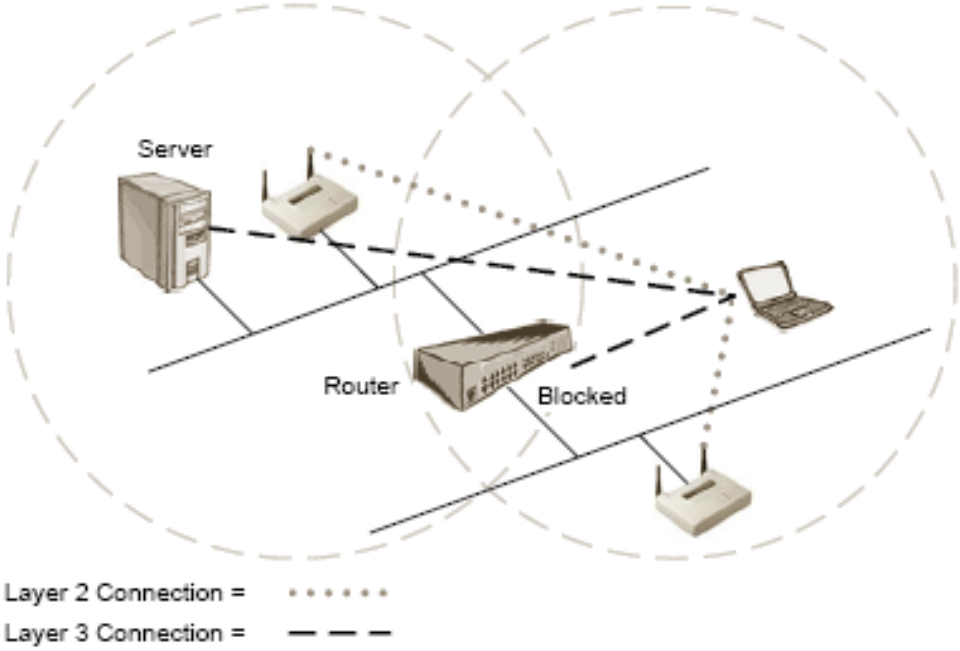


Cisco in Persian

Roaming within VPN tunnels

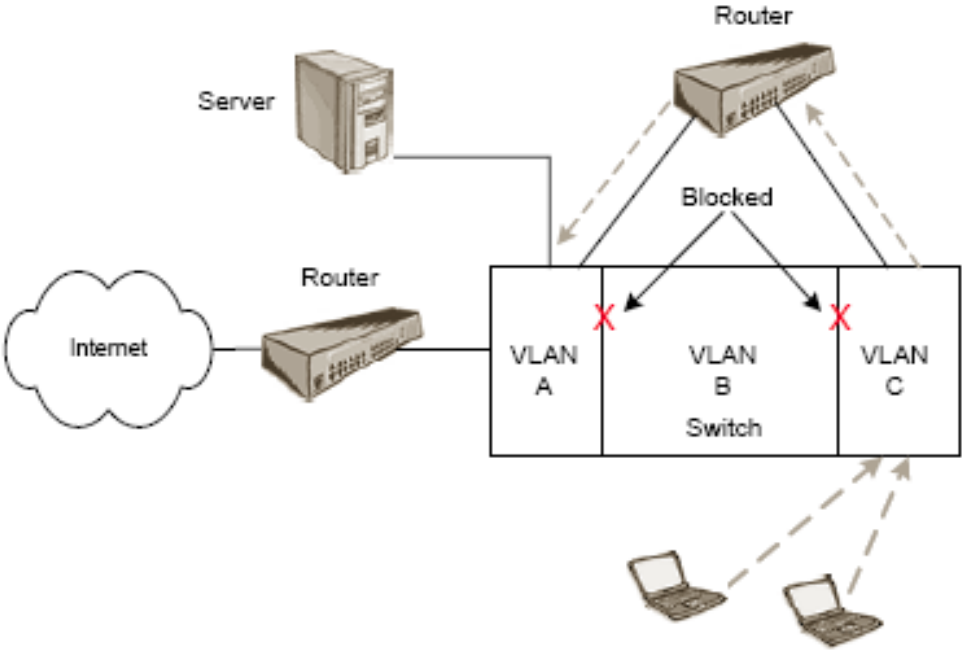


Roaming across Layer 3 boundaries



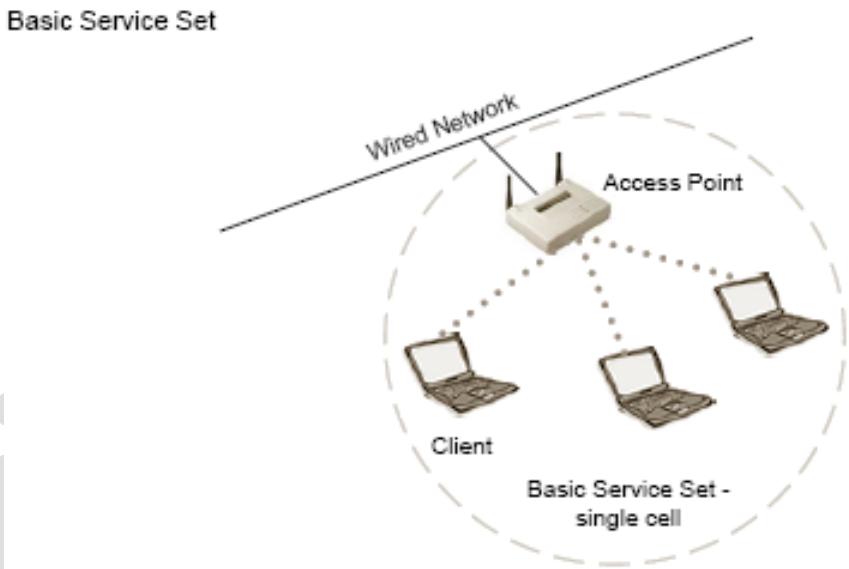
Cisco in Persian

Roaming Across VLANs

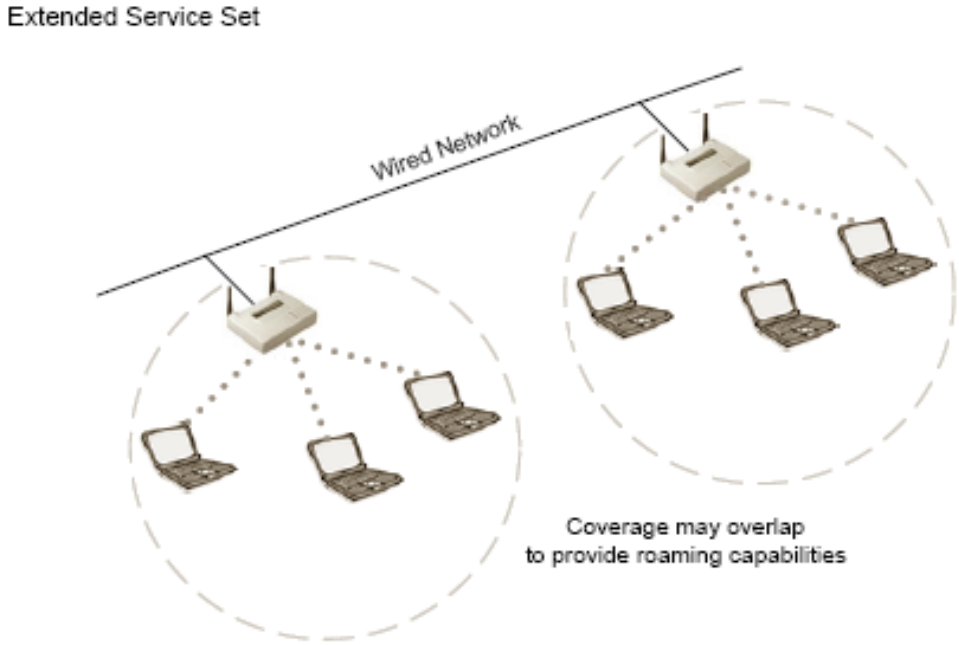


توپولوژی های 802.11 – انواع Service Set

- **BSS (Basic Service Set)** : BSS یا مدل Infrastructure ، برای موقعیست که چند Station به یک AP متصل می شوند و تمامی ترافیک شبکه از طریق AP مبادله خواهد شد و ارتباط فیزیکی مستقیم Client به Client مجاز نیست . یک BSS دارای یک SSID یکتا خواهد بود و یک سلول (Cell) یا RF Zone را دربر می گیرد و Client با توجه به فاصله و مدار قرارگیری نسبت به AP ، پهنای باندی معادل 1, 2, 5.5, 11 Mbps را خواهد داشت.



- **ESS (Extended Service Set)** : ESS شامل دو یا چند BSS است که توسط یک سیستم توزیع به هم وصل شده اند و چندین Cell را شامل شده و roaming را ارائه می دهند .



Cisco in Persian

- **IBSS (Independent Basic Service Set)** : IBSS یا Ad hoc از AP استفاده نمی کند ، اما در کل شبکه همه Station ها از یک SSID استفاده می کنند و خود Client ها موظف به ارسال Beacon هستند . در این روش یکی از Client ها می تواند Gateway به دنیای بیرون باشد . به این روش Peer to Peer نیز می گویند .

Independent Basic Service Set

Cisco in Persian

فصل هفتم : تجهیزات وایرلس

Cisco in Persian

- ❖ انواع Access Point
  - ✓ Root Mode
  - ✓ Bridge
  - ✓ Repeater
- ❖ انواع Wireless Bridge
  - ✓ Root Bridge
  - ✓ Non-root
  - ✓ Repeater
  - ✓ Access Point
- ❖ Wireless Workgroup Bridge
- ❖ Wireless Residential Gateway
- ❖ Wireless LAN Clients

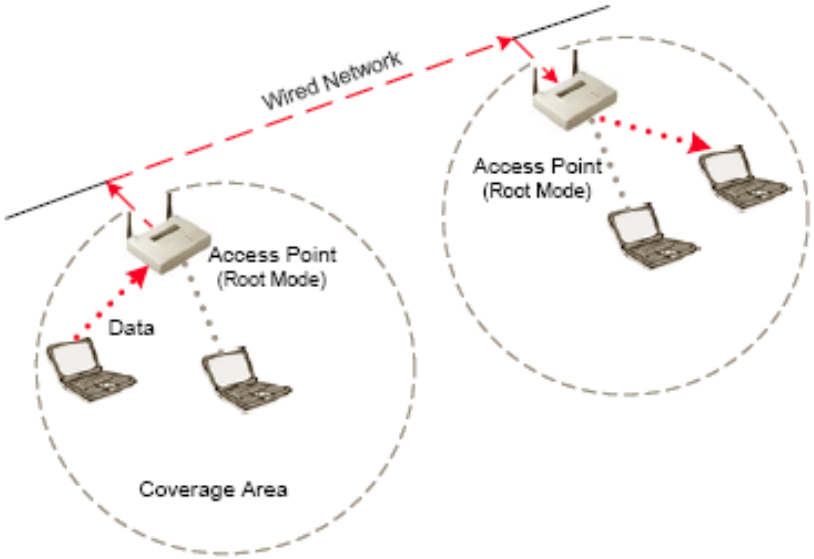
انواع Access Point

یک AP را می توان به سه گونه به کار گرفت :

۱. Root Mode

چند Client بی سیم بوسیله AP به هم و به شبکه LAN متصل می شوند.

An access point in root mode

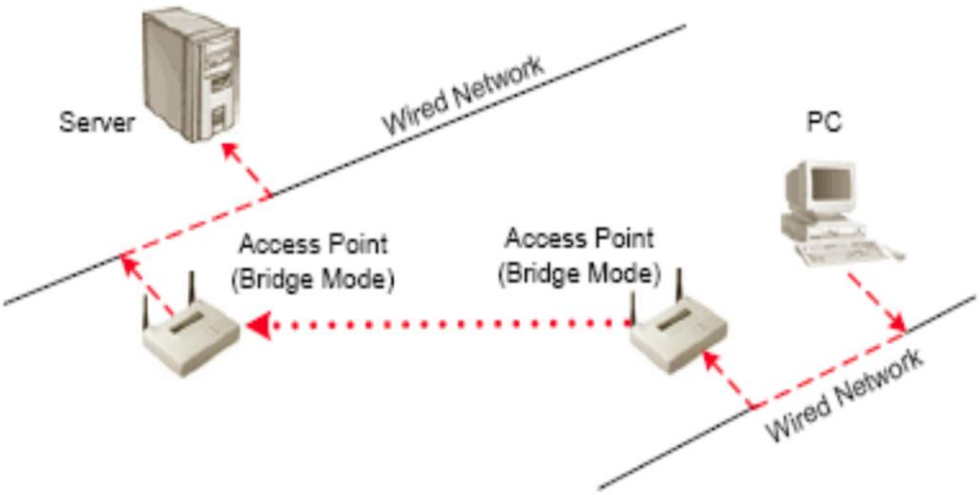


Cisco in Persian

۲. Bridge

دو شبکه سیمی (Wired) را به هم متصل می کند . AP هایی که قابلیت Bridge دارند ، گران قیمت ترند.

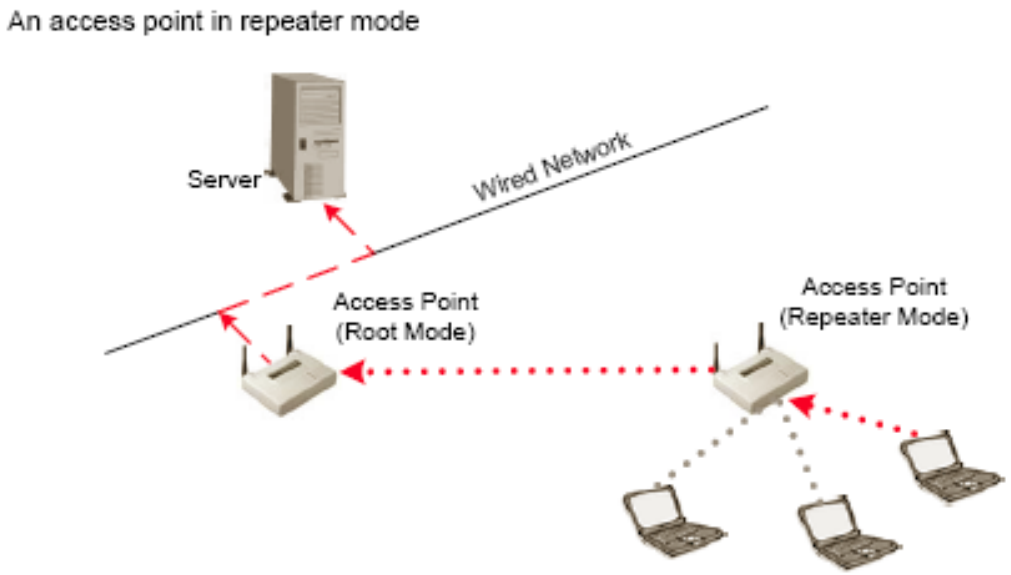
An access point in bridge mode



[A جدا]

۳. Repeater

AP شبکه بی سیم خود را به AP دیگر (Root) متصل می کند.



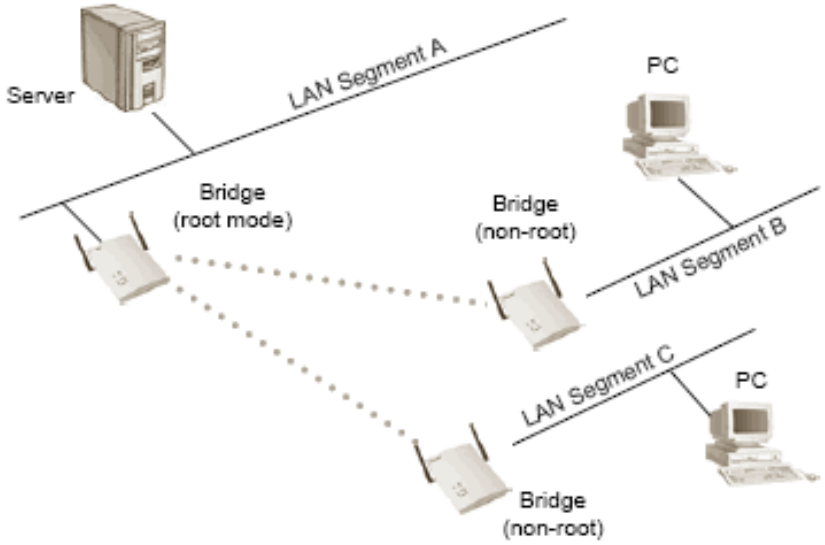
Cisco in Persian

انواع Wireless Bridge

۱. Root Bridge

متصل کننده دو Bridge دیگر به خود می باشد ؛ یعنی دو LAN دیگر نیز از طریق آن به هم متصل می شوند.

A root bridge communicating with non-root bridges



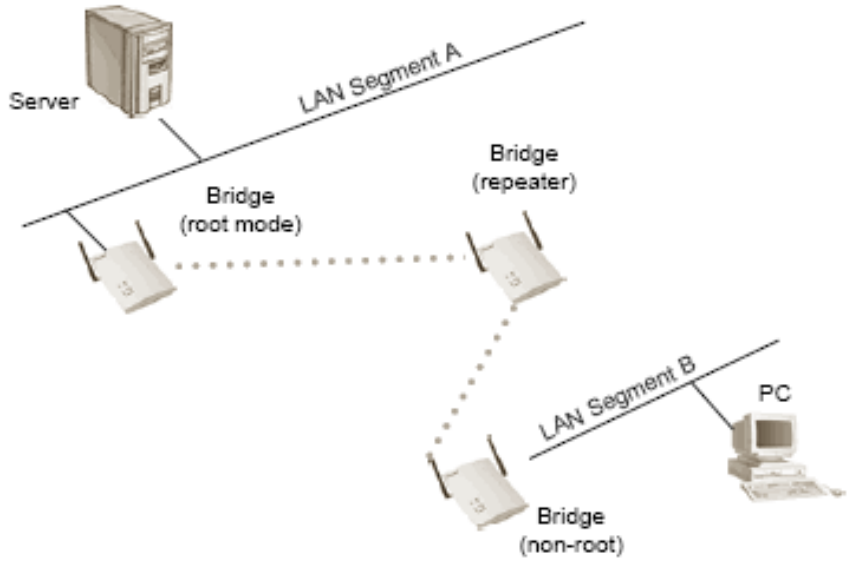
۲. Non-root

به Root متصل می شود و Bridging می کند.

۳. Repeater

دو شبکه Wireless را به هم متصل می کند و از پورت LAN خود استفاده نمی کند .

A wireless bridge in repeater mode



Cisco in Persian

۴. Access Point

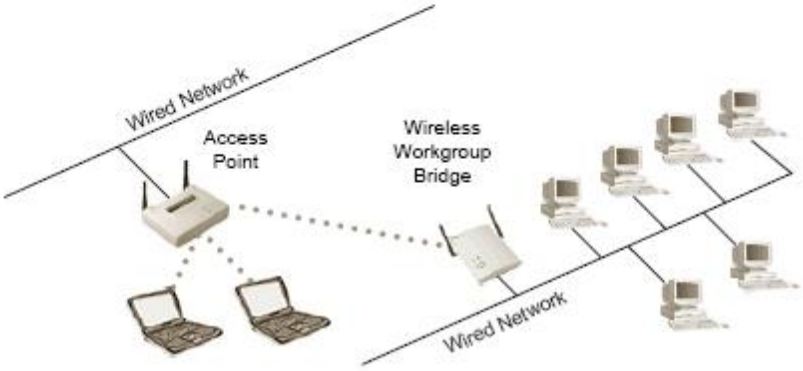
در این حالت ، علاوه به Bridging ، AP هم هست و کاربران بصورت بی سیم به آن متصل و Associate میشوند.

Wireless Workgroup Bridge

تنها یک Client برای شبکه بی سیم است که یک شبکه LAN را به یک AP متصل کرده و از آدرس MAC خود بجای آدرس کامپیوترهای LAN استفاده می کند .

A sample wireless workgroup bridge

A wireless workgroup bridge installed on a network



Wireless Residential Gateway

دارای خصوصیات متنوعی می باشد نظیر اتصال Cable-XDSL-Satellite Modem-Leased Line و در عین حال بعنوان AP ، کار به اشتراک گذاردن اینترنت ، L3 Routing ، DHCP ، PPPoE و ... را انجام می دهد.

Wireless LAN Clients

انواع PCI ، ISA ، USB و ... را شامل می شود که در اصل یا PCMCIA و یا CF (Compact Flash) است و بقیه کارتها مبدل یکی از این دو گونه به USB یا PCI هستند .

فصل هشتم : WLAN Deployment و کاربردهای آن

- ❖ کاربردهای WLAN
  - ✓ Access Role
  - ✓ Network Extension
  - ✓ Building to Building Connectivity
  - ✓ Last Mile Data Delivery
  - ✓ Mobility
  - ✓ SOHO
  - ✓ Mobile Offices

Cisco in Persian

کاربرد ها

در این بخش ، به کاربرد های مختلف Wireless LAN می پردازیم .

Access Role

Wireless LAN یک نوع روش دسترسی به شبکه است و در لایه Data-Link کار می کند. WISP هایی هستند که از Wireless در لایه Distribution استفاده می کنند که این فرکانس ها همیشه فرکانسهای مجزا و دارای مجوز می باشند.

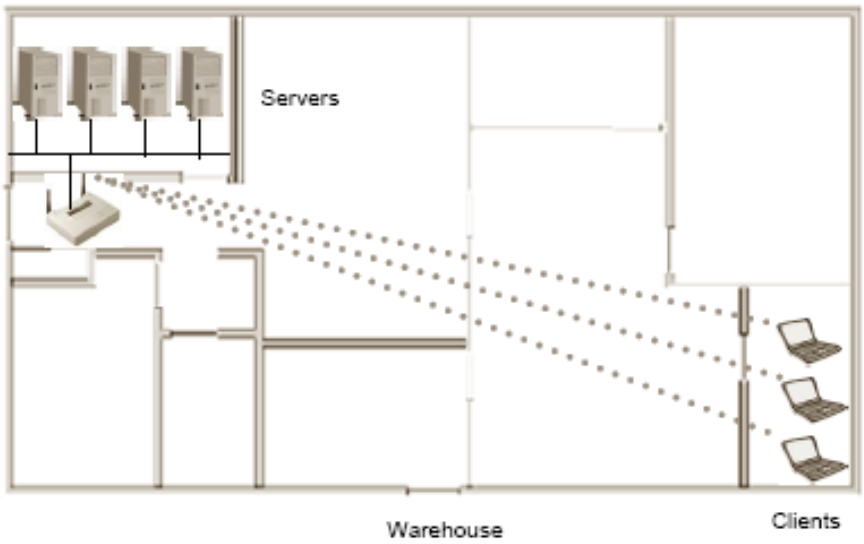
Access role of a wireless LAN

Cisco in Persian

Network Extension

می توان جهت افزایش پوشش یک شبکه LAN از WLAN استفاده کرد.

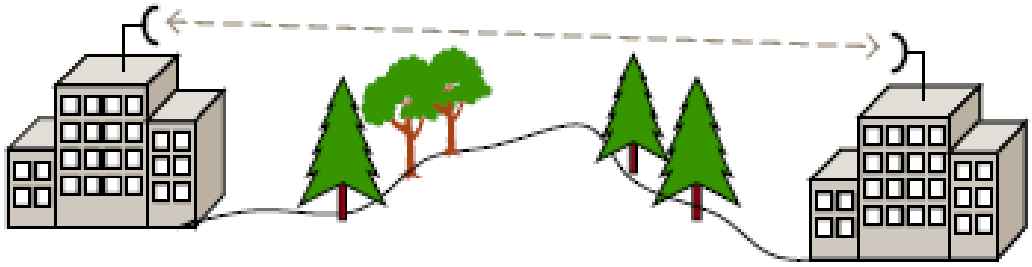
Network Extension



Building to Building Connectivity

در گذشته ، برای ارتباط دو ساختمان از کابل (اغلب در زیر زمین) استفاده می شد یا از Leased Line ؛ که می توان بجای آن از ارتباط بی سیم استفاده کرد . این ارتباط می تواند PTP (Point to Point) و یا PTMP (Point to Multi-Point) باشد ، که در PTP آنتن ها اغلب از نوع Semi-Directional و یا Highly-Directional هستند.

Building-to-building connectivity



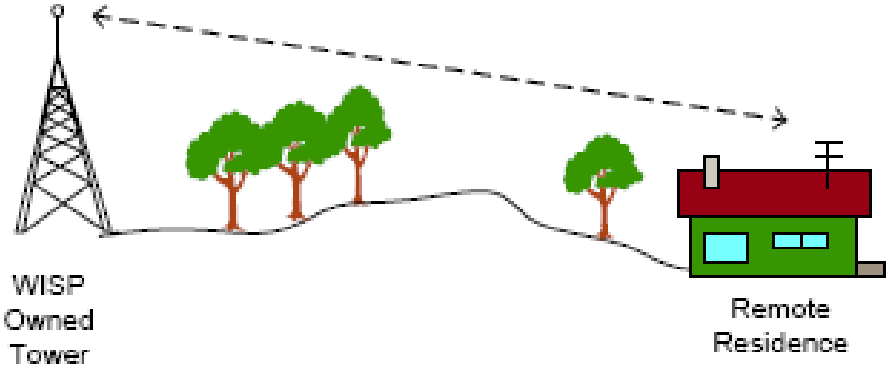
در PTMP ارتباط بین چند نقطه است که عموما بشکل ستاره ای (Hub and Spoke) و یک ساختمان در مرکز اجرا می شود. در این موارد از آنتن های Omni-directional در مرکز و Semi-directional در نقاط اطراف استفاده می شود.

Cisco in Persian

Last Mile Data Delivery

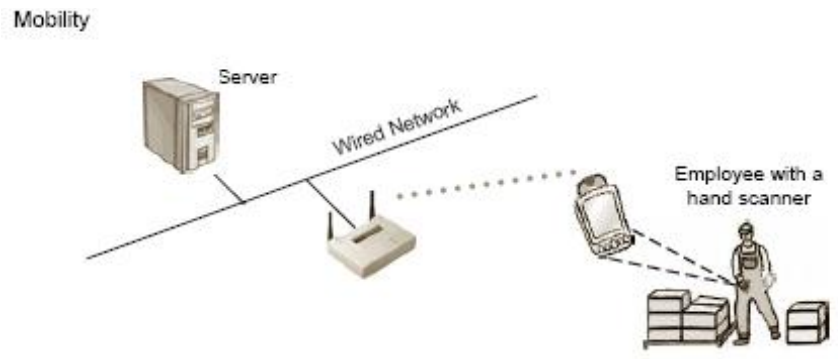
در واقع Last Mile ، ارتباط بین Telco تا End-user است که می تواند با کابل و یا بی سیم باشد.

Last Mile Service



Mobility

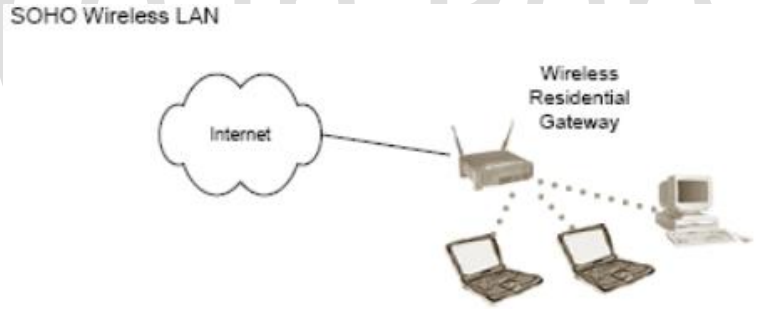
خصوصیت قابل حرکت بودن و در عین حال اتصال به شبکه از دیگر ویژگی های بارز شبکه بی سیم است.

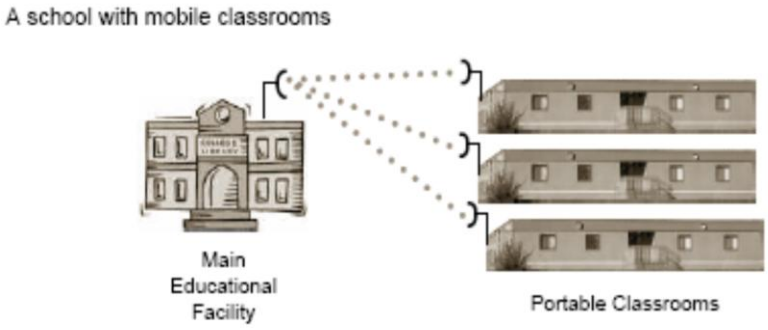


Small Office – Home Office

بدون نیاز به سیم کشی و ایجاد سوراخ در دیوارهای منازل یا دفاتر کار ، می توان محیط کار یا منزل را شبکه کرد.

Cisco in Persian



Mobile Offices

استفاده شبکه بی سیم در کنفرانس ها، کلاس های درس، همایش ها، بیمارستان ها و مزایای منحصر بفرد آن از دیگر دلایل همه گیر شدن این تکنولوژی است.